



HiPER 840G Gigabit Router

Advanced Configuration Guide

V1.0

Copyright Notice

Copyright © 2000-2013. UTT Technologies Co., Ltd. All rights reserved.

Information in this document, including URL and other Internet Web site references, is subject to change without further notice.

Unless otherwise noted, the companies, organizations, people and events described in the examples of this document are fictitious, which have no relationship with any real company, organization, people and event.

Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or used for any commercial and profit purposes, without the express prior written permission of UTT Technologies Co., Ltd.

UTT Technologies Co., Ltd. has the patents, patent applications, trademarks, trademark applications, copyrights and other intellectual property rights that are mentioned in this document. You have no license to use these patents, trademarks, copyrights or other intellectual property rights, without the express prior written permission of UTT Technologies Co., Ltd.

艾泰[®] and UTT[®] are the registered trademarks of Technologies Co., Ltd.

HiPER[®] is the registered trademark of UTT Technologies Co., Ltd.

Unless otherwise announced, the products, trademarks and patents of other companies, organizations or people mentioned herein are the properties of their respective owners.

Product Number (PN): 0904-0101-001

Document Number (DN): PR-PMMU-1150.50-PPR-EN-1.0A

Table of Contents

Copyright Notice.....	2
Table of Contents.....	I
About This Manual.....	1
0.1 Scope	1
0.2 Web UI Style.....	1
0.3 Documents Conventions	2
0.3.1 Symbol Conventions	2
0.3.2 Other Conventions	2
0.3.3 Common Button Descriptions	2
0.3.4 Detailed Description of List	3
0.4 Factory Default Settings	5
0.5 Document Organization.....	5
0.6 Contact Information	8
Chapter 1 Product Overview	9
1.1 Product Brief.....	9
1.2 Key Features	9
1.3 Physical Specification.....	10
Chapter 2 Hardware Installation.....	11
2.1 Physical Characteristics	11
2.1.1 Front Panel	11
2.1.2 Rear Panel	13
2.2 Installation Procedure.....	13
Chapter 3 Quick Setup	15
3.1 Configuring Your Computer	15
3.2 Logging in to the Gigabit Router.....	17
3.3 Setup Wizard.....	19
3.3.1 Running the Setup Wizard	19
3.3.2 Setup Wizard - Internet Access Mode	
3.3.3 Setup Wizard - Internet Connection Settings	20
3.3.4 Setup Wizard - Wireless Settings	
Chapter 4 Start Menu.....	24
4.1 Setup Wizard	24

4.2	System Status	24
4.2.1	Wired Status	24
4.2.2	Wireless Status	25
4.3	Interface Traffic	27
4.4	Restart	29
Chapter 5	Network	30
5.1	WAN Settings	30
5.1.1	Internet Connection List	30
5.1.2	Internet Connection Settings	34
5.1.3	MAC Address Clone	40
5.2	Load Balancing	41
5.2.1	Introduction to Load Balancing and Failover	41
5.2.2	Load Balancing Global Settings	43
5.2.3	Load Balancing List	44
5.2.4	Connection Detection Settings	45
5.2.5	How to Configure Connection Detection Settings	47
5.3	LAN Settings	48
5.4	DHCP Server	49
5.4.1	DHCP Server Settings	49
5.4.2	Static DHCP	51
5.4.3	DHCP Client List	53
5.4.4	Configuration Example for DHCP	55
5.5	DDNS	58
5.5.1	Introduction to DDNS	58
5.5.2	Apply for a DDNS Account	58
5.5.3	DDNS Settings	59
5.5.4	DDNS Status	61
5.5.5	DDNS Verification	62
5.6	UPnP	63
5.6.1	Enable UPnP	63
5.6.2	UPnP Port Forwarding List	63
Chapter 6	Advanced	65
6.1	NAT and DMZ	65
6.1.1	Introduction to NAT Features	65
6.1.2	Port Forwarding	68
6.1.3	NAT Rule	71
6.1.4	DMZ	77
6.2	IP/MAC Binding	79
6.2.1	Introduction to IP/MAC Binding	79
6.2.2	IP/MAC Binding Global Settings	80
6.2.3	IP/MAC Binding List	81
6.2.4	IP/MAC Binding Settings	82

6.2.5	How to Add IP/MAC Bindings	83
6.2.6	Internet Whitelist and Blacklist	84
6.3	Static Route	87
6.3.1	Introduction to Static Route	87
6.3.2	Static Route List	87
6.3.3	Static Route Settings	88
6.3.4	How to Add Static Routes	89
6.4	PPPoE Server	91
6.4.1	PPPoE Overview	91
6.4.2	PPPoE Server Global Settings	93
6.4.3	PPPoE Account List	94
6.4.4	PPPoE Account Settings	94
6.4.5	PPPoE User Status	95
Chapter 7	User Management	97
7.1	Global Management	97
7.1.1	Global Management Policy Settings	97
7.1.2	An Example for Global Management Policy	99
7.2	Group Management	100
7.2.1	Group Management Policy List	100
7.2.2	Group Management Policy Settings	101
7.2.3	Execution Order of Group Management Policies	103
7.2.4	Priorities of Global and Group Management Policies and Access Rules	103
7.2.5	An Example for Group Management Policy	103
Chapter 8	Firewall	108
8.1	Access Control	108
8.1.1	Introduction to Access Control	108
8.1.2	Access Rule List	110
8.1.3	Access Rule Settings	111
8.1.4	Configuration Examples for Access Rule	116
8.2	Domain Filtering	122
8.2.1	Domain Filtering Global Settings	122
8.2.2	Domain Filtering Settings	122
8.3	Attack Prevention	124
Chapter 9	VPN	125
9.1	Introduction to PPTP Implementation	125
9.1.1	Protocol Overview	126
9.1.2	Packet Flow - PPTP Client	127
9.1.3	User Authentication	128
9.1.4	Data Confidentiality	128
9.1.5	MTU and Fragmentation	128
9.1.6	PPTP Sessions Limit	130

9.2	PPTP Client Settings	130
9.3	PPTP Client List	131
9.4	Configuration Example for PPTP Client	132
9.5	IPSEC VPN	174
9.5.1	Introduction to IPsec Implementation.....	174
9.5.2	IPsec Settings–AutoKey (IKE)	190
9.5.3	IPsec List	200
9.5.4	How to Add, View, Edit and Delete IPsec Entries	201
9.5.5	Configuration Examples for IPsec – AutoKey (IKE).....	202
Chapter 10	System Administration	134
10.1	Administrator	134
10.1.1	Administrator List	134
10.1.2	Administrator Settings.....	135
10.2	System Time.....	136
10.3	Configuration	138
10.3.1	Backup Configuration	138
10.3.2	Restore Configuration	138
10.3.3	Reset to Factory Defaults	139
10.4	Firmware Upgrade.....	140
10.5	Remote Access.....	142
10.6	Scheduled Task	143
10.6.1	Scheduled Task Settings	143
10.6.2	Scheduled Task List.....	144
Chapter 11	Status	145
11.1	System Status	145
11.2	Traffic Statistics	147
11.3	System Information	148
Chapter 12	Support	150
Appendix A	How to Configure Your PC	151
Appendix B	FAQ	155
1.	How to connect the Gigabit Router to the Internet using PPPoE?.....	155
2.	How to connect the Gigabit Router to the Internet using Static IP?	156
3.	How to connect the Gigabit Router to the Internet using DHCP?	156
4.	How to reset the Gigabit Router to factory default settings?	158
Appendix C	Common IP Protocols	159
Appendix D	Common Service Ports	160
Appendix E	Figure Index	165

Appendix F Table Index.....	169
------------------------------------	------------

About This Manual

0.1 Scope

This guide mainly describes how to install and configure the HiPER 840G Gigabit Router offered by UTT Technologies Co., Ltd. For more information, please visit our website at www.uttglobal.com.

0.2 Web UI Style

The Web UI style complies with the browser standard, which is as follows: 

Radio Button: It allows you to choose only one of a predefined set of options. 

Check Box: It allows you to choose one or more options.



Button: It allows you to click to perform an action.



Text Box: It allows you to enter text information.



List Box: It allows you to select one or more items from a list contained within a static, multiple line text box.



Drop-down List: It allows you to choose one item from a list. When a drop-down list is inactive, it displays a single item. When activated, it drops down a list of items, from which you may select one.

0.3 Documents Conventions

0.3.1 Symbol Conventions

◆: It represents a configuration parameter. Parameters may be optional or required. Required parameters are indicated by a red asterisk (*).

▶: It represents a button.

✓: It represents one or more notes.

0.3.2 Other Conventions

0.3.2.1 Convention for a Page Path

First Level Menu Item > Second Level Menu Item (bold font) means the menu path to open a page. For example, **Network > DHCP Server** means that in the Web UI, click the first level menu item **Network** firstly, and then click the second level menu item **DHCP Server** to open the corresponding page.

0.3.2.2 Convention for Clicking a Button

Click the **XXX** button (**XXX** is the name of the button, bold font) means performing the corresponding operation. E.g., click the **Delete** button means performing the delete operation, the **Delete** button is shown as .

0.3.3 Common Button Descriptions

The following table describes the commonly-used buttons in the Web UI.

Button	Description
	Click to save your changes.

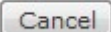
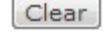
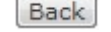
	Click to revert to the last saved settings.
	Click to delete the selected entry(s).
	Click to display the latest information on the page.
	Click to clear all the statistics on the page.
	Click to go back to the previous page.

Table 0-1 Common Button Descriptions

0.3.4 Detailed Description of List

0.3.4.1 Basic Elements and Features

The Web UI contains two kinds of lists: editable list and read-only list.

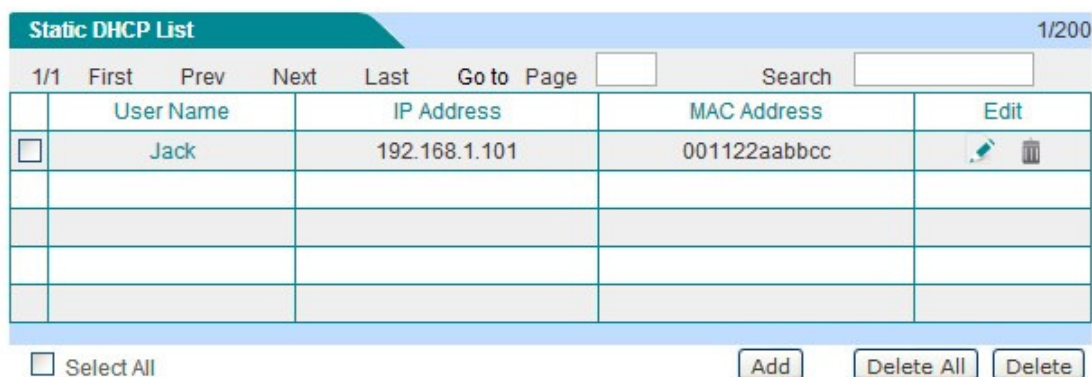
- An editable list is used to add, display, modify and delete the configuration entries.
- A read-only list is used to display the system status information which is not editable.

Let's take the editable **Static DHCP List** (see Figure 0-1) as an example to explain the basic elements and features of the list.



Note

Only the editable lists support Add, Modify, and Delete operations. The read-only lists don't support them.



Static DHCP List 1/200

1/1 First Prev Next Last Go to Page Search

	User Name	IP Address	MAC Address	Edit
☐	Jack	192.168.1.101	001122aabbcc	 

☐ Select All Add Delete All Delete

Figure 0-1 MAC Address Filtering List

The following table describes the basic elements and features of the list.

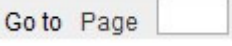
Element	Description
	Current page number/ total pages, the example means that the current page is the first page, and total one page.
	Click to jump to the first page.
	Click to jump to the previous page.
	Click to jump to the next page.
	Click to jump to the last page.
	Enter page number in text field, then click Go to or press <Enter> key to jump to that page.
	Enter the text string you want to search for in this text box, then press <Enter> key to display all the matched entries. In addition, you can do the search within the displayed results. If you want to display all the entries, you only need clear the text box and then press <Enter> key. Note that the matching rule is substring matching, that is, it will search for and display those entries that contain the specified text string.
	Configured number / maximum number, the example means that there is 1 configured DHCP Static entries, and the maximum number of DHCP Static entries allowed is 100.
	Click to go to the setup page to modify the corresponding entry.
	Click to delete the corresponding entry.
	Click (add the check mark) to select all the entries in the current page. Click again (remove the check mark) to unselect all the entries in the current page.
	Click to go to the setup page to add a new entry to the list.
	Click to delete all the entries in the list.
	To delete one or more entries, select the leftmost check boxes of them, and then click the Delete button.

Table 0-2 Basic Elements and Features of the List

0.3.4.2 Sorting Function

All the lists in the Web UI support sorting function. The operation is as follows: You can click any column header to sort the entries in a list by that column. Click once to sort the entries in descending order, click again to sort them in ascending order. Click a third time to sort them in descending order, and so forth. After sorted, the list will be displayed from the first page.

0.4 Factory Default Settings

The following table lists the default values of several important parameters.

Parameter	Default Value	Description
Administrator User Name	admin	You can use the administrator account to login to the Gigabit Router's Web UI. Note: Both the User Name and Password are case sensitive.
Administrator Password	admin	
LAN IP Address	192.168.1.1	They are the IP address and subnet mask of the Gigabit Router's LAN interface. You can use this IP address to access and manage the Gigabit Router.
LAN Subnet Mask	255.255.255.0	

Table 0-3 Factory Default Settings

0.5 Document Organization

This guide mainly describes the settings and applications of the HiPER 840G Gigabit Router, which include product overview, hardware installation, quick setup, start menu, network, wireless, advanced, user management, firewall, VPN, system administration, status and support.

Chapter 1 Product Overview

This chapter describes functions and features of the Gigabit Router.

Chapter 2 Hardware Installation

This chapter describes how to install the Gigabit Router.

Chapter 3 Quick Setup

This chapter describes the following contents:

- How to install and configure TCP/IP properties on your PC.
- How to login to the Gigabit Router; and introduction to the WEB UI layout.
- How to use the **Setup Wizard** to quickly configure the basic parameters for the Gigabit Router to operate properly.

Chapter 4 Start Menu

This chapter describes how to quickly go to the following pages to configure the related features via the **Start** menu items:

- **Setup Wizard:** How to configure the basic parameters for the Gigabit Router to operate properly.
- **System Status:** How to view wired and wireless status of the Gigabit Router.
- **Interface Traffic:** How to view the real-time traffic chart for each interface, and the ingress and egress traffic statistics for each interface.
- **Restart:** How to restart the Gigabit Router.

Chapter 5 Network

This chapter describes how to configure the basic network parameters of the Gigabit Router, including:

- **WAN:** How to configure Internet connections and view their configuration and status.
- **Load Balancing:** How to configure the load balancing feature which includes detection and weight settings, global settings; and how to view the load balancing list.
- **LAN Settings:** How to configure the parameters of the LAN interface, such as IP address, subnet mask, MAC address, and so on.
- **DHCP Server:** How to configure DHCP server, DNS proxy, static DHCP; how to view the static DHCP list and DHCP client list.
- **DDNS:** How to apply for DDNS account and configure DDNS service, and view DDNS status.
- **UPnP:** How to enable or disable UPnP, and view the UPnP port forwarding list.

Chapter 6 Advanced

This chapter describes how to configure the advanced features of the Gigabit Router, including:

- **NAT and DMZ:** How to configure and view NAT rules, port forwarding entries and DMZ host.
- **IP/MAC Binding:** How to configure IP/MAC bindings to prevent IP address spoofing. How to configure an Internet whitelist or blacklist for the LAN users.

- **Static Route:** How to configure and view the static routes.
- **PPPoE Server:** How to configure PPPoE server global settings and PPPoE account settings, and view PPPoE user status.

Chapter 7 User Management

This chapter describes how to control and manage the Internet behaviors of the LAN users based on schedule, including:

- **Global Management:** How to allow or block the LAN users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., Bit Comet, Bit Spirit, Thunder Search) based on schedule.
- **Group Management:** How to allow or block the LAN users from using popular IM and P2P applications based on user group and schedule.

Chapter 8 Firewall

This chapter describes how to configure firewall features, including:

- **Access Control:** How to configure access control rules to assign Internet access privileges to the LAN users based on schedule, and to prevent external attacks.
- **Domain Filtering:** How to configure domain filtering feature to block access to the specified websites.
- **Attack Prevention:** How to configure attack prevention features.

Chapter 9 VPN

This chapter describes the PPTP implementation, and how to configure the Gigabit Router as a PPTP client.

Chapter 10 System Administration

This chapter describes how to perform maintenance activities on the Gigabit Router, including:

- **Administrator:** How to add, view, modify and delete the administrator accounts.
- **System Time:** How to set the system date and time manually or automatically.
- **Configuration:** How to backup and restore the system configuration, and reset the Gigabit Router to factory default settings.
- **Firmware upgrade:** How to backup, download and upgrade firmware.
- **Remote Access:** How to enable HTTP remote management feature to remotely configure and manage the Gigabit Router via Internet.
- **Scheduled Task:** How to create and view the scheduled tasks. Now the Gigabit Router only supports one scheduled task: Restart.

Chapter 11 Status

This chapter describes how to view the system status information and statistics, including:

- **System Status:** It displays wired and wireless status of the Gigabit Router.
- **Traffic Statistics:** It displays wired and wireless data traffic statistics of the Gigabit Router.
- **System Information:** It displays the current system time, system up time, system resources usage information, SN, firmware version, and system log messages.

Chapter 12 Support

This chapter describes how to link to the UTTCare, Forum, Knowledge and Reservation page of the UTT website, which can help you quickly learn the UTT Technologies service system and enjoy the most intimate and professional services.

Appendix

This guide provides six appendixes, including:

- **Appendix A How to Configure Your PC:** How to configure TCP/IP settings on a Windows XP-based computer.
- **Appendix B FAQ:** Frequent questions and answers.
- **Appendix C Common IP Protocols:** Provides the list of common IP protocols and their protocol numbers.
- **Appendix D Common Service Ports:** Provides the list of common services and their port numbers.
- **Appendix E Figure Index:** Provides a figure index directory.
- **Appendix F Table Index:** Provides a table index directory.

0.6 Contact Information

If you have any questions regarding the operation or installation of the HiPER 840G Gigabit Router, please contact us in any of the following ways.

- **Technical Skype Support :** [uttglobal](#)
- **UTT Forum:** <http://www.uttglobal.com/forum/>
- **E-mail:** uttglobal@utt.com.cn

Chapter 1 Product Overview

Thanks for choosing the HiPER 840G Gigabit Router from UTT Technologies Co., Ltd. This chapter describes the functions and features of the HiPER 840G Gigabit Router in brief.

1.1 Product Brief

HiPER 840G Gigabit Router is designed for small-sized businesses and branch offices, integrating wired networks network. In addition, it adheres to the characteristics of UTT Technologies products: open, easy-to-use, safe, smooth, and so on.

The HiPER 840G supports DHCP server, NAT, static route, DDNS, IP/MAC binding, PPPoE server and other advanced features. Furthermore, it provides feature-rich user management, which can help you control and manage the Internet behaviors of the LAN users based on schedule and address group, including MSN and P2P applications (e.g., Bit Comet, Bit Spirit, and Thunder Search) control, the maximum upload and download rate limiting.

The HiPER 840G supports flexible firewall features like access control and domain filtering to effectively prevent network attacks, and provide security for the LAN users.

The HiPER 840G provides a concise, intuitive, and feature-rich Web User Interface. The Setup Wizard can help you quickly configure the basic parameters for the Gigabit Router to operate properly. The status information (System Status, Traffic Statistics, etc.) can help you identify and diagnose the source of current system problems, or predict potential system problems. In addition, the Support page provides links to the UTT website to help you quickly learn the UTT Technologies service system and enjoy the most intimate and professional services.

1.2 Key Features

- Supports multiple Internet connection types: PPPoE, Static IP, DHCP
- Provides 4 wired WAN ports (WAN1~WAN4), and 1 LAN port
- Supports multiple Internet connections that provide intelligent load balancing and automatic failover

- Supports 6kV lightning protection
- Supports VPN pass-through (IPSec, PPTP and L2TP)
- Supports PPTP client
- Supports DHCP server
- Supports DNS proxy
- Supports DDNS (Dynamic Domain Name System)
- Supports IP/MAC binding
- Supports feature-rich PPPoE server
- Supports upload and download rate limiting for the LAN users
- Supports Internet behavior management for the LAN users, such as block or allow QQ, MSN and P2P applications (e.g., Bit Comet, Bit Spirit, and Thunder Search)
- Supports flexible and strong firewall features
- Supports IP packet filtering based on IP address, protocol and TCP/UDP port
- Supports URL and keyword filtering
- Supports DNS request filtering
- Supports HTTP remote management
- Provides the Web User Interface (Web UI) for ease of use
- Supports firmware upgrade via the Web UI
- Supports configuration backup and restore
- Provides wireless client list and system status

1.3 Physical Specification

- Conforms to IEEE 802.3 Ethernet and IEEE 802.3u Fast Ethernet standards
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, Static Route, Tag-based VLAN etc.
- Each physical port supports auto-negotiation for the port speed and duplex mode
- Each physical port supports auto MDI/MDI-X
- Provides system and port LEDs
- Operating Environment:
 - Temperature: 32 °F to 104 °F (0 °C to 40 °C)
 - Relative Humidity: 10% to 90%, Non-condensing
 - Height: 0m to 4000m

Chapter 2 Hardware Installation

2.1 Physical Characteristics

2.1.1 Front Panel

As shown in Figure 2-1, the LEDs are located on the front panel of the Gigabit Router. The LEDs indicate the status of the system and each port. Table 2-1 describes these LEDs.

The front panel also offers a Reset button, a USB port and 5 ports. Table 2-2 describes these ports.

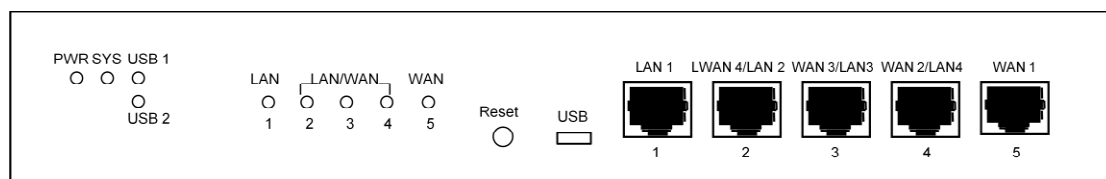


Figure 2-1 Front Panel of the Gigabit Router

1. LEDs

LED	Full Name	State	Description
PWR	Power LED	On	The Gigabit Router is powered on.
		Off	The Gigabit Router is powered off.
SYS	System LED	Blinking	The system is operating properly.
		On	The system is not operating properly.
		Off	The system is not operating properly.
USB 1	Built-in USB Status LED	On	There's 1 built-in USB Flash Memory connected to the system.

		Off	There's no built-in USB Flash Memory connected to the system.
USB 2	USB Status LED	On	There's 1 USB Flash Memory connected to the system.
		Off	There's no USB Flash Memory connected to the system.
WAN1	WAN1 Port Status LED	On	A valid link is established on the corresponding port.
		Blinking	The corresponding port is sending or receiving data.
		Off	No link is established on the corresponding port.
WAN2/LAN 4, WAN3/LAN3, WAN4/LAN2	WAN/LAN Ports Status LED	On	A valid link is established on the corresponding port.
		Blinking	The corresponding port is sending or receiving data.
		Off	No link is established on the corresponding port.
LAN 1,	LAN Port Status LED	On	A valid link is established on the corresponding port.
		Blinking	The corresponding port is sending or receiving data.
		Off	No link is established on the corresponding port.

Table 2-1 Description of LEDs on the Front Panel

2. Reset Button

If you forget the administrator password, you need to use the Reset button to reset the Gigabit Router to factory default settings. The operation is as follows: While the Gigabit Router is powered on, use a pin or paper clip to press and hold the Reset button for more than 5 seconds, and then release the button. After that, the Gigabit Router will restart with factory default settings.



Note

This operation will clear all the custom settings on the Gigabit Router. If you remember the administrator account, it is strongly recommended that you go to **Administration > Configuration** page to backup the current configuration firstly, and then reset the Gigabit Router to factory default settings.

3. Ports

The Gigabit Router provides 1 LAN port, 4 WAN ports by Default, and a USB port. Table 2-2 describes these ports. Please note that this Device can be set to different LAN/WAN.

Port	Description
LAN	They are used to connect the wired computers, hubs, switches, and other Ethernet network devices on the LAN to the Gigabit Router.
WAN1 ~ WAN4	They are used to connect the Gigabit Router to the Internet.
USB	The Gigabit Router provides a USB port for connecting a 3G USB Modem, which is used to connect the Gigabit Router to the Internet.

Table 2-2 Description of Ports on the Rear Panel

2.1.2 Rear Panel

As shown in Figure 2-2, the rear panel of the Gigabit Router contains a POWER connector and a power switch.



Figure 2-2 Back Panel of the Gigabit Router

Component	Number	Description
Power	1	It is used to connect the power adapter.
Power Switch	1	It is used to switch on or off the Device

Table 2-3 Description of Components on the Rear Panel

2.2 Installation Procedure

1. Selecting a Proper Location

Please make sure that the Gigabit Router is powered off before installing it. Then you

need to select a proper location to install the Gigabit Router. In most cases, you can install it on a level surface such as a desktop or shelf.

**Note**

Please ensure that the desktop or shelf is stable and the power outlet is grounded properly, and do not place heavy objects on the Gigabit Router.

2. Connecting the Gigabit Router to the LAN

Connect a standard network cable from a PC or switch to a LAN port of the Gigabit Router, or connect a PC to the Gigabit Router wirelessly. The Gigabit Router will automatically adapt to any network device operating at 10Mbps or 100Mbps.

3. Connecting the Gigabit Router to the Internet

Connect the network cable provided by the manufacturer from the DSL, cable or fiber optic modem to a WAN port of the Gigabit Router, or insert your 3G USB modem to the USB port of the Gigabit Router.

4. Powering On the Gigabit Router

Connect the supplied power cord to the power connector on the rear panel of the Gigabit Router, and then plug the other end of the power cord to a grounded power outlet. The Gigabit Router will start automatically.

**Note**

To prevent the Gigabit Router from working abnormally or being damaged, please make sure that the power supply and connectivity are normal, and the power outlet is grounded properly before powering on the Gigabit Router.

5. Checking the LEDs

Verify that the Gigabit Router starts up properly and the network connections are operational by checking the LED states, as described in Table 2-1.

Chapter 3 Quick Setup

This chapter describes how to properly configure TCP/IP settings on your computer, how to login to the Gigabit Router, and how to configure the basic parameters to quickly connect the Gigabit Router to the Internet via the **Start > Setup Wizard**. In addition, it also briefly describes the layout and style of the Gigabit Router's Web UI.

3.1 Configuring Your Computer

Before configuring the Gigabit Router via the Web UI, you should properly configure TCP/IP settings on the computer that you use to administer the Gigabit Router. To do this, follow these steps:

- Step 1** Connect the computer to a LAN port of the Gigabit Router.
- Step 2** Install TCP/IP protocol on your computer. If it has been installed, please ignore it.
- Step 3** Configure TCP/IP settings on your computer: set the computer's IP address to an IP address in the range of 192.168.1.2 through 192.168.1.254, set its subnet mask to 255.255.255.0, set its default gateway to 192.168.16.1 (the Gigabit Router's default LAN IP address is 192.168.1.1 with a subnet mask of 255.255.255.0), and set its DNS server to an available IP address provided by your ISP.
- Step 4** To verify the network connection between your computer and the Gigabit Router, you can use the ping command at the command prompt on the computer: **Ping 192.168.1.1**
- If the displayed page is similar to the screenshot below, the connection between your computer and the Gigabit Router has been established.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- If the displayed page is similar to the screenshot below, the connection between your computer and the Gigabit Router hasn't been established yet.

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

If the connection hasn't been established, please take the following steps to resolve the problem:

1. Is the physical link between your computer and the Gigabit Router connected properly?

Verify that the LED corresponding to the Gigabit Router's LAN port and the LED on your computer's adapter are lit.

2. Is the TCP/IP configuration for your PC correct?

Verify that your computer is on the same subnet as the Gigabit Router's LAN interface. For example, if the Gigabit Router's LAN IP address is 192.168.1.1/24 (default value), your computer's IP address must be an IP address in the range of 192.168.1.2 through 192.168.1.254, which is not being used by another network device; and its default gateway must be 192.168.1.1.

3.2 Logging in to the Gigabit Router

This section describes how to login to the Gigabit Router.

No matter what operating system is installed on your computer, such as, MS Windows, Macintosh, UNIX, or Linux, and so on, you can login to and configure the Gigabit Router through the Web browser (for example, Internet Explorer).

To login to the Gigabit Router, do the following: Open a Web browser, enter the Gigabit Router's LAN interface IP address (the default is **192.168.1.1**) in the address bar, and then press **<Enter>** key, see Figure 3-1.

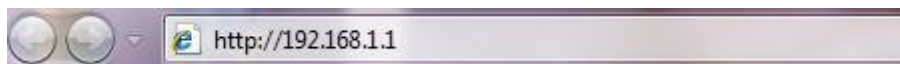


Figure 3-1 Entering IP address in the Address Bar

A login screen prompts you for your user name and password, see Figure 3-2. When you first login to the Gigabit Router, please use the default administrator account: Enter **admin** in both the **User name** and **Password** boxes (the default user name and password both are **admin**), lastly click **OK**.

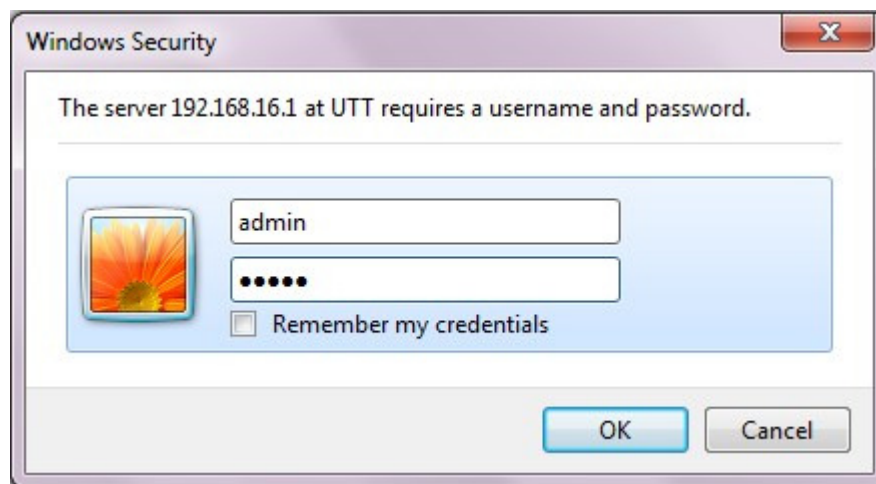


Figure 3-2 Login Screen

If your user name and password are correct, it will display the homepage, see Figure 3-3.

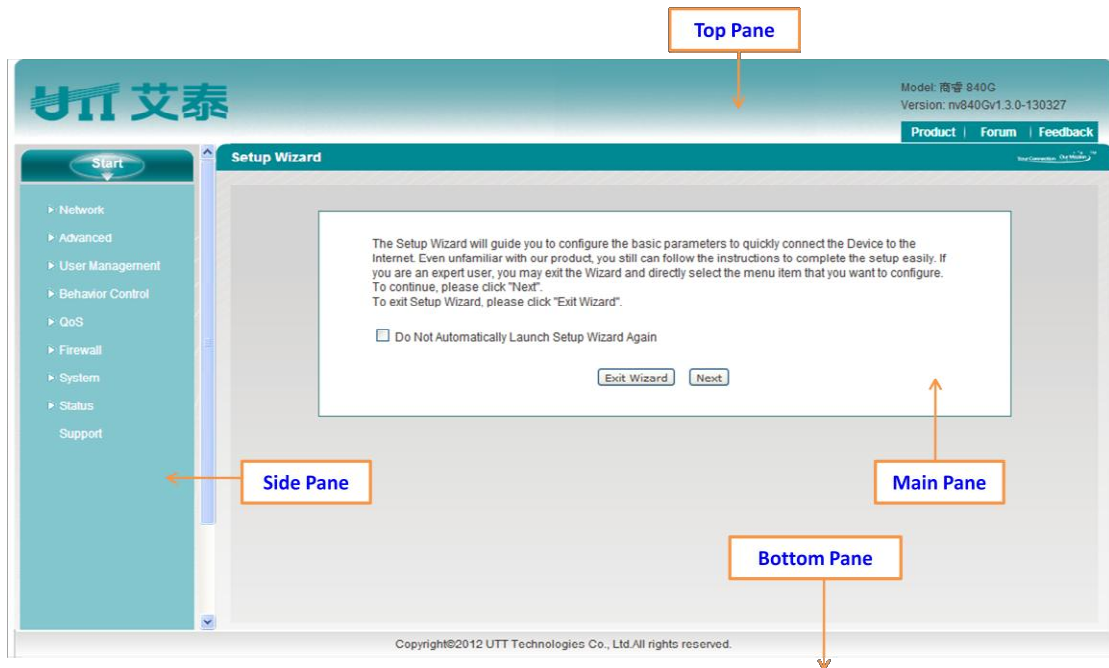


Figure 3-3 Homepage

Each page of the Gigabit Router's Web UI consists of four panes:

1. **Top Pane:** It displays UTT logo, model and version, and three shortcut icons.
 - 1) **UTT Logo:** Click to link to the homepage of the UTT website.
 - 2) **Model and Version:** The product model and firmware version of the Gigabit Router.
 - 3) **Short Icons:** They are used for fast link to the corresponding pages on the website of UTT Technologies Co., Ltd.
 - **Product:** Click to link to the products page of the UTT website to find more products.
 - **Forum:** Click to link to the forum homepage of the UTT website to participate in product discussions.
 - **Feedback:** Click to link to send us your feedback by E-mail.
2. **Main Pane:** It is the location where you can configure each feature of the Gigabit Router, view configuration, status and statistics.
3. **Side Pane:** It displays the two-level main menu bar (i.e., navigation bar). The first level menu is always visible. The second level menu is hidden by default. You can click a first level menu item to reveal its submenu items, click again to hide them.
4. **Bottom Pane:** It displays copyright information.

If this is the first time that you login to the Gigabit Router, the first page of the **Setup Wizard** appears. In the next section we will describe how to use the **Setup Wizard** to configure the basic parameters for the Gigabit Router to operate properly.

3.3 Setup Wizard

This section describes the **Start > Setup Wizard** page.

3.3.1 Running the Setup Wizard

As mentioned earlier, the first page of the **Setup Wizard** appears immediately after your first login, see the following figure.

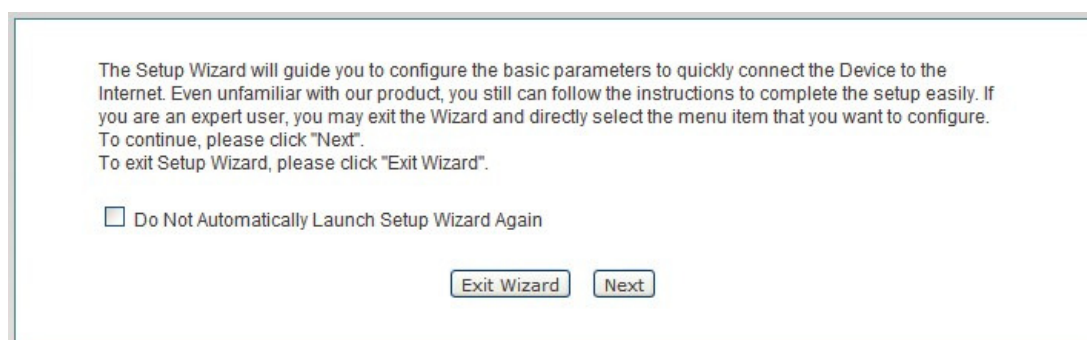


Figure 3-4 Running the Setup Wizard

- ◆ **Do Not Automatically Launch the Wizard Again:** If you select this check box, the system don't automatically launch the **Setup Wizard** the next time you login to the Gigabit Router, instead directly open the **Welcome** page shown in Figure 3-5. Else, the system will still launch the **Setup Wizard** automatically.
- ▶ **Exit Wizard:** Click to exit the **Setup Wizard** and go to the **System > System Information** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**, that is, the **Setup Wizard - WAN1 Settings** page shown in 错误！未找到引用源。。

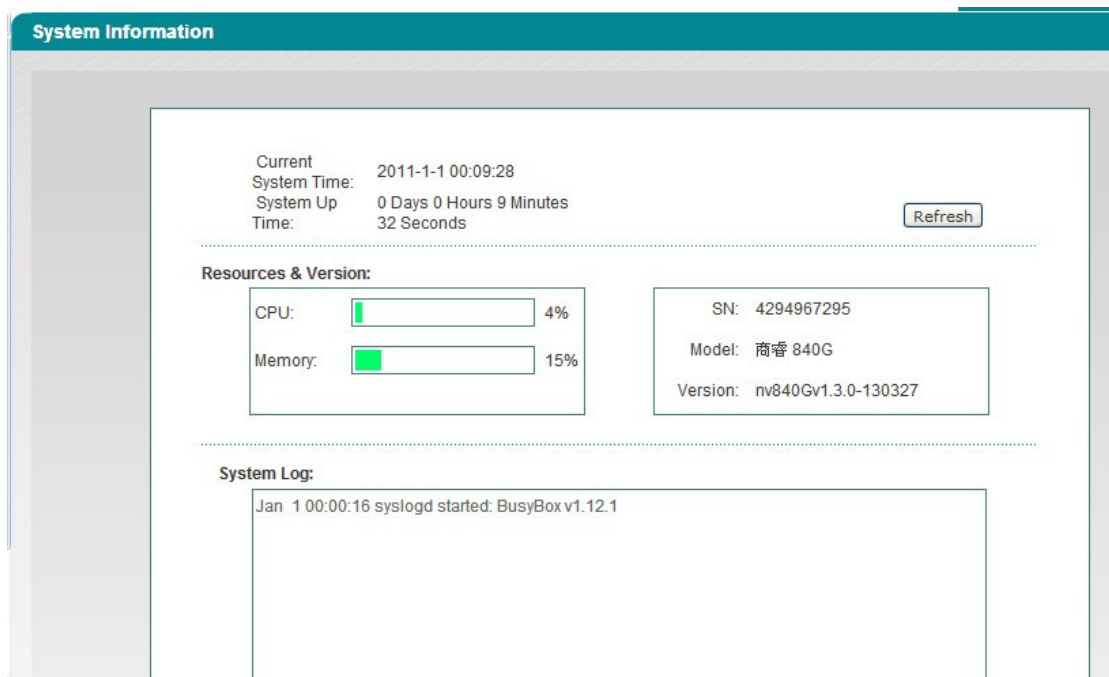


Figure 3-5 Welcome Page

3.3.2 Setup Wizard - WAN1 Internet Connection Settings

In the **Setup Wizard**, you can configure each Internet connection respectively. For each Internet access mode, the Internet connection settings are different.

For the WAN1 Internet connection, there are three connection types: PPPoE, Static IP and DHCP.

3.3.2.1 Static IP Internet Connection Settings

If you are required to use a static IP address, please select **Static IP** from the **Connection Type** drop-down list. Then the following page will be shown.

Here you can configure the WAN1 connection as required.

Connection Type	Static IP ▼
IP Address*	200.200.200.12
Subnet Mask*	255.255.255.0
Default Gateway*	200.200.200.254
Primary DNS Server*	202.96.209.5
Secondary DNS Server	

Figure 3-6 Setup Wizard - WAN1 Internet Connection Settings (Static IP)

- ◆ **Connection Type:** It specifies the type of the Internet connection. Here please select **Static IP**. You need to manually configure IP address, subnet mask, default gateway and DNS server addresses, which are provided by your ISP.
- ◆ **IP Address:** It specifies the IP address of the WAN interface, which is provided by your ISP.
- ◆ **Subnet Mask:** It specifies the subnet mask of the WAN interface, which is provided by your ISP.
- ◆ **Default Gateway:** It specifies the IP address of the default gateway, which is provided by your ISP.
- ◆ **Primary DNS Server:** It specifies the IP address of your ISP's primary DNS server.
- ◆ **Secondary DNS Server:** It specifies the IP address of your ISP's secondary DNS server. If it is available, you may set it. Else, please leave it blank.
- ▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- ▶ **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**.



Note

The WAN IP address and default gateway IP address must be on the same subnet. If not, please modify the **Subnet Mask** to make them be on the same subnet. If you don't have the subnet related knowledge, please ask a professional or UTT customer

engineer for help.

3.3.2.2 DHCP Internet Connection Settings

If your ISP automatically assigns an IP address to the Gigabit Router via DHCP, please select **DHCP** from the **Connection Type** drop-down list. Then the following page will be shown.

Here you can configure the WAN1 connection as required.

Connection Type

Figure 3-7 Setup Wizard - WAN1 Settings (DHCP)

- ◆ **Connection Type:** It specifies the type of the Internet connection. Here please select **DHCP**. The Gigabit Router will automatically obtain the WAN IP address, subnet mask and gateway and DNS server addresses from your ISP's DHCP server.
- ▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- ▶ **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**.

3.3.2.3 PPPoE Internet Connection Settings

Please select **PPPoE** from the **Connection Type** drop-down list if your ISP uses PPPoE to establish the Internet connection for you. Then the following page will be shown.

Here you can configure the WAN1 connection as required.

Connection Type

User Name*

Password*

Figure 3-8 Setup Wizard - WAN1 Settings (PPPoE)

- ◆ **Connection Type:** It specifies the type of the Internet connection. Here please select **PPPoE**. The Gigabit Router will automatically obtain the WAN IP address, subnet mask and gateway IP address from your ISP's PPPoE server.
- ◆ **User Name** and **Password:** They specify the PPPoE login user name and password provided by your ISP. Please ask your ISP if you have any questions.
- ▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- ▶ **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- ▶ **Next:** Click to go to the next page of the **Setup Wizard**.

Chapter 4 Start Menu

The **Start** menu item is the first one under the top-level menu. It provides links to several commonly used pages including **Setup Wizard**, **System Status**, **Interface Traffic** and **Restart**, where you can quickly configure the basic parameters for the Gigabit Router to operate properly, view system status, view interface traffic statistics, and restart the Gigabit Router.

4.1 Setup Wizard

The **Start > Setup Wizard** can help you configure the basic parameters for the Gigabit Router to operate properly. Refer to **Section 3.3 Setup Wizard** for detailed information.

4.2 System Status

This section describes the **Start > System Status** page, where you can view the current status information of the Gigabit Router.

4.2.1 Wired Status

This page displays the current status information of the wired interfaces, which include WAN1 and LAN.

Wired Status

Wireless Status

WAN1:

Connection Type	PPPoE	Status	Connected
IP Address	114.62.0.46	Subnet Mask	255.255.255.255
Gateway IP Address	114.62.0.1	MAC Address	00:22:AA:A8:A7:83
Primary DNS Server	219.233.241.166	Secondary DNS Server	211.167.97.67
Up Time	0:5:17:50		

WAN2:

Connection Type	DHCP	Status	Disconnected
IP Address		Subnet Mask	
Default Gateway		MAC Address	00:22:AA:A8:B1:94
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		

LAN:

IP Address	192.168.1.1	Subnet Mask	255.255.255.0
MAC Address	00:22:AA:A8:9D:73		

Refresh

Figure 4-1 System Status - Wired Status

- ◆ **WAN1:** It displays the current status and basic configuration of the WAN1 Internet connection, which include connection type, status, IP address, subnet mask, MAC address, default gateway and DNS server addresses, and up time.
- ◆ **LAN:** It displays the basic configuration of the LAN interface, which include IP address, subnet mask and MAC address.
- ▶ **Refresh:** Click to view the latest wired status information.

4.2.2 Wireless Status

This page displays the current status information of the wireless interfaces, which include 3G, APClient and Wireless LAN.

Wired Status

Wireless Status

3G:

Connection Type

3G

Status

Disconnected

IP Address

Subnet Mask

Gateway IP Address

MAC Address

Primary DNS Server

Secondary DNS Server

Up Time

0:0:0:0

APClient:

Connection Type

DHCP

Status

Disconnected

IP Address

Subnet Mask

Default Gateway

MAC Address

00:22:AA:A8:C5:B9

Primary DNS Server

Secondary DNS Server

Up Time

0:0:0:0

Wireless LAN:

Status

Enabled

Operation Mode

APClient Mode

SSID

UTT-HIPER_a89d73

Wireless Mode

11b/g/n Mixed

Channel

6

MAC Address

00:22:AA:A9:B0:1C

Refresh

Figure 4-2 System Status - Wireless Status

- ◆ **3G:** It displays the current status and basic configuration of the 3G Internet connection, which include connection type, status, IP address, subnet mask, MAC address, default gateway and DNS server addresses, and up time.
- ◆ **APClient:** It displays the current status and basic configuration of the APClient Internet connection, which are the same as those of the 3G Internection connection.
- ◆ **Wireless LAN:** It displays the current status and basic configuration of the Wireless LAN, which include status, operation mode, SSID, wireless mode, channel and MAC address.
- ▶ **Refresh:** Click to view the latest wireless status information.

**Note**

The **Wired Status** page and **Wireless Status** page only display the status

information of the interfaces that have been configured.

4.3 Interface Traffic

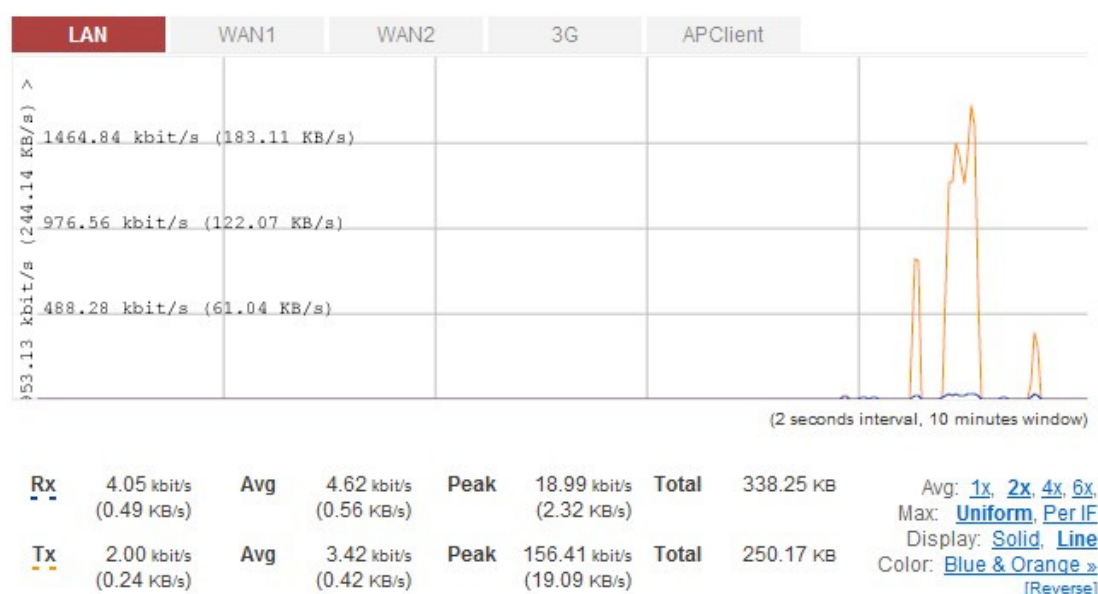
This section describes the **Start > Interface Traffic** page.

This page provides the real-time traffic chart for each interface that has been configured, which displays the real-time Rx/Tx rate, average Rx/Tx rate, maximum Rx/Tx rate and total Rx/Tx traffic of each interface. For example, as shown in Figure 4-3, all of the Gigabit Router's interfaces (LAN, WAN1, 3G and APClient) have been configured.



Note

If the SVG Viewer plug-in isn't installed on your web browser, the port traffic chart cannot be displayed properly. Please click the **(Please install SVG Viewer if the page cannot be displayed properly.)** hyperlink to download and install the SVG Viewer to view the traffic chart.



[\(Please install SVG Viewer if the page cannot be displayed properly.\)](#)

[View Traffic Statistics](#)

Figure 4-3 Interface Traffic Chart

- ◆ **Avg: 1x, 2x, 4x, 6x:** It specifies the number of samples to average, or no averaging.
- ◆ **Max:** It determines that the charts are scaled uniformly to the max traffic value of all interfaces or individually per interface.
- ◆ **Display:** It allows you to change the type of chart displayed. The options are **Line** and **Solid**.

- **Line:** Select this option to display a line chart. The chart includes two lines with different colors, which represent the real-time Rx rate and Tx rate respectively.
 - **Solid:** Select this option to display an area chart. The area chart is like the line chart except that the area between the axis the plot line is solid.
- ◆ **Color:** It specifies the colors of the two lines (or filled areas), such as red, blue, black, etc.
- ◆ **Reverse:** Click to toggle the colors of the two lines (or filled areas).
- ▶ **LAN, WAN1, APClient and 3G:** You can select an interface name at the top to view the traffic chart for that interface.
- ▶ **View Traffic Statistics:** Click to view the ingress and egress traffic statistics for the interfaces that have been configured, see Figure 4-4.

WAN1:		Transmitted	Received
	Bytes	2305372	7971015
	Packets	10327	11409
3G:		Transmitted	Received
	Bytes	0	0
	Packets	0	0
LAN:		Transmitted	Received
	Bytes	9780001	2604198
	Packets	11797	10647
		Clear	Refresh
		Back	

Figure 4-4 Traffic Statistics

- ◆ **WAN1, 3G, APClient and LAN:** You can view the traffic statistics for each interface, including the number of bytes received and transmitted, and the number of packets received and transmitted.
- ▶ **Clear:** Click to clear all traffic statistics.
- ▶ **Refresh:** Click to view the latest traffic statistics.
- ▶ **Back:** Click to go back to the **Start > Interface Traffic** page.

**Note**

This page only displays the traffic statistics for the interfaces that have been configured.

4.4 Restart



Figure 4-5 Restart the Gigabit Router

- ▶ **Restart:** Click to restart the Gigabit Router.

If you click the **Restart** button, the system will pop up a prompt dialog box (see Figure 4-6). Then you can click **OK** to restart the Gigabit Router, or click **Cancel** to cancel the operation.

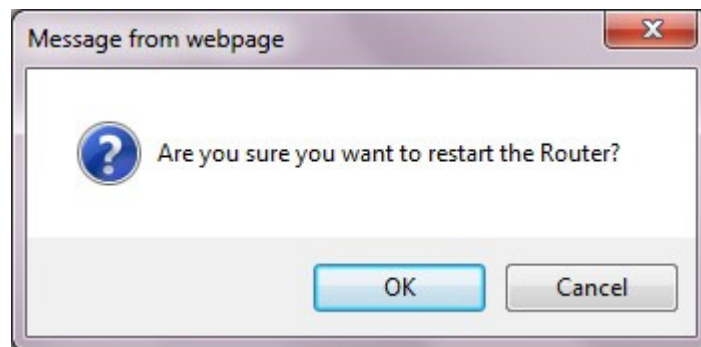


Figure 4-6 Prompt Dialog Box - Restart the Gigabit Router

✓ Note

Restarting the Gigabit Router will disconnect all the sessions, so please do it with caution.

Chapter 5 Network

This chapter describes how to configure the basic network parameters of the Gigabit Router, which include WAN settings, load balancing, LAN settings, DHCP server, DDNS, and UPnP.

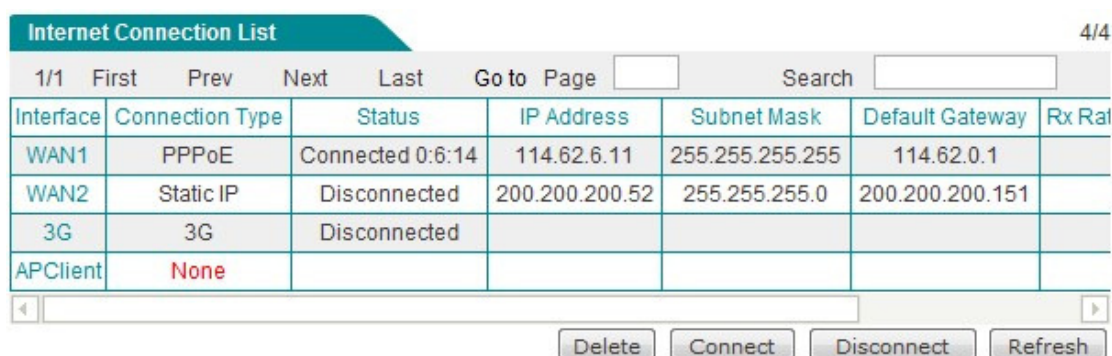
5.1 WAN Settings

This section describes the **Network > WAN** page.

If you have configured one or more Internet connections in the **Start > Quick Wizard**, you can view their configuration and status in this page, and modify or delete them if needed. You also can directly configure one or more Internet connections in this page.

5.1.1 Internet Connection List

You can view the configuration and status of each Internet connection in the **Internet Connection List**, see Figure 5-1.



Internet Connection List							4/4
1/1	First	Prev	Next	Last	Go to Page	Search	
Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate	
WAN1	PPPoE	Connected 0:6:14	114.62.6.11	255.255.255.255	114.62.0.1		
WAN2	Static IP	Disconnected	200.200.200.52	255.255.255.0	200.200.200.151		
3G	3G	Disconnected					
APClient	None						

Delete Connect Disconnect Refresh

Figure 5-1 Internet Connection List

Internet Connection List							4/4
1/1	First	Prev	Next	Last	Go to	Page	Search
Status	IP Address	Subnet Mask	Default Gateway	Rx Rate (KB/s)	Tx Rate (KB/s)	Edit	
Connected 0:6:14	114.62.6.11	255.255.255.255	114.62.0.1	0	0		
Disconnected	200.200.200.52	255.255.255.0	200.200.200.151	0	0		
Disconnected				0	0		
							

Figure 5-2 Internet Connection List (Continue)

5.1.1.1 Parameter Definitions

- ❖ **Interface:** It displays the name of the WAN interface. The Gigabit Router has four WAN interfaces: WAN1, 3G, and APClient. Therein, WAN1 are wired interfaces, and 3G and APClient are wireless interfaces.
- ❖ **Connection Type:** It displays the type of the Internet connection. There are four connection types: Static IP, PPPoE, DHCP and 3G.
- ❖ **Status:** It displays current status of the connection. There are four cases:

1. PPPoE Connection Status

For the PPPoE connection, there are two kinds of status, see Table 5-1. When it is connected, it will also display the elapsed time (days: hours: minutes: seconds) since connected.

Status	Description
Disconnected	The connection is disconnected due to that the interface is disabled or not connected, or the Gigabit Router doesn't dial up yet, or wrong user name or password, etc.
Connected	Authentication succeeded, and the connection is established and ready for data transmission.

Table 5-1 Description of PPPoE Connection Status

2. Static IP Connection Status

For the static IP connection, there are two kinds of status, see Table 5-2.

Status	Description
--------	-------------

Disconnected	The connection is disconnected due to that the interface is disabled or not connected, etc.
Connected	The connection is established between the Gigabit Router and peer device.

Table 5-2 Description of Static IP Connection Status

3. DHCP Connection Status

For the DHCP connection, there are two kinds of status, see Table 5-3. When it is connected, it will also display the elapsed time (days: hours: minutes: seconds) since connected.

Status	Description
Disconnected	The connection is disconnected due to that the interface is disabled or not connected, or the Gigabit Router has released the IP address but hasn't obtained a new one yet, etc.
Connected	The Gigabit Router has obtained an IP address, and the connection is established successfully.

Table 5-3 Description of DHCP Connection Status

4. 3G Connection Status

For the 3G connection, there are two kinds of status, see Table 5-4. When it is connected, it will also display the elapsed time (days: hours: minutes: seconds) since connected.

Status	Description
Disconnected	The connection is disconnected due to that the 3G USB modem isn't inserted properly, or wrong ISP, 3G USB modem settings, etc.
Connected	The Gigabit Router has obtained an IP address, and the connection is established successfully.

Table 5-4 Description of 3G Connection Status

◆ **IP Address, Subnet Mask and Default Gateway:** They display the current IP settings of the connection. There are two cases:

- For the PPPoE, DHCP or 3G Internet connection, it will show the current WAN IP address, subnet mask and gateway IP address which are assigned by your ISP.
- For the static IP Internet connection, it will show the information you have entered manually.

- ◆ **Rx Rate:** It displays the average download speed (in kilobytes per second) of the Internet connection during the time interval between two refresh operations.
- ◆ **Tx Rate:** It displays the average upload speed (in kilobytes per second) of the Internet connection during the time interval between two refresh operations.

5.1.1.2 How to Add, View, Modify and Delete Internet Connections

- ▶ **Add an Internet Connection:** To add a new Internet connection, first click its **Interface** hyperlink or  icon, and then configure it, lastly click the **Save** button.
- ▶ **View Internet Connection(s):** When you have configured one or more Internet connections, you can view them in the **Internet Connection List**.
- ▶ **Modify an Internet Connection:** To modify a configured Internet connection, click its **Interface** hyperlink or  icon, the related information will be displayed in the setup fields. Then modify it, and click the **Save** button.
- ▶ **Delete an Internet Connection:** To delete an Internet connection, click its **Interface** hyperlink or  icon to select the connection, and then click the **Delete** button below the list.
- ▶ **Refresh Internet Connection List:** To view the latest status of the Internet connections, click the **Refresh** button below the list.

5.1.1.3 How to Connect and Disconnect a PPPoE/3G Connection

If you click the **Interface** hyperlink or  icon of a PPPoE or 3G connection, the **Connect** and **Disconnect** button will appear below the list, see Figure 5-3.

If the PPPoE connection's **Dial Type** is set to **Manual** (see **Section 5.1.2.1.3 PPPoE Internet Connection Settings**), you need to click the **Connect** button to connect it, and click the **Disconnect** button to disconnect it.

- ▶ **Connect:** Click to connect the PPPoE or 3G Internet connection manually.
- ▶ **Disconnect:** Click to disconnect the PPPoE or 3G Internet connection manually.

Internet Connection List							4/4
1/1	First	Prev	Next	Last	Go to Page		Search
Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate	
WAN1	PPPoE	Connected 0:9:2	114.62.6.11	255.255.255.255	114.62.0.1		
WAN2	DHCP	Disconnected	200.200.200.52	255.255.255.0			
3G	3G	Disconnected					
APClient	None						

Figure 5-3 Internet Connection List - PPPoE/3G Connection

5.1.1.4 How to Renew and Release a DHCP Connection

If you click the **Interface** hyperlink or  icon of a DHCP connection, the **Renew** button and **Release** button will appear below the list, see Figure 5-4.

Internet Connection List							4/4
1/1	First	Prev	Next	Last	Go to Page		Search
Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate	
WAN1	PPPoE	Connected 0:10:2	114.62.6.11	255.255.255.255	114.62.0.1		
WAN2	DHCP	Disconnected					
3G	3G	Disconnected					
APClient	None						

Figure 5-4 Internet Connection List - DHCP Connection

- **Renew:** Click to re-obtain an IP address from the ISP's DHCP server. The Gigabit Router will automatically release the assigned IP address firstly, and then obtain a new IP address from the DHCP server.
- **Release:** Click to release the IP address obtained from the ISP's DHCP server.

5.1.2 Internet Connection Settings

If you want to configure an Internet connection, please click its **Interface** hyperlink or  icon in the **Internet Connection List**. The setup page is shown in Figure 5-5.

Internet Connection List

4/4

1/1

First

Prev

Next

Last

Go to Page

Search

Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate
WAN1	PPPoE	Connected 0:11:15	114.62.6.11	255.255.255.255	114.62.0.1	
WAN2	DHCP	Disconnected				
3G	3G	Disconnected				
APClient	None					

Delete

Renew

Release

Refresh

Interface

WAN2

Connection Type

DHCP

ISP Policy

None

Save

Cancel

Figure 5-5 Network - WAN Settings

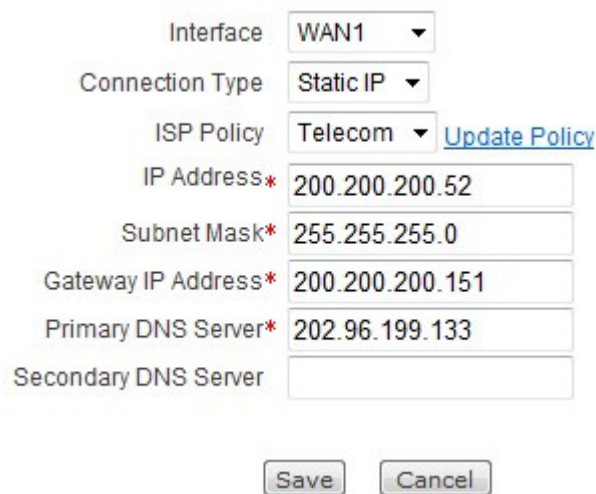
**Note**

1. It allows you to choose the **ISP Policy** (i.e., route policy database) for each Internet connection. The system will automatically create the associated static routes according to your selection. Thus all traffic destined for one ISP's servers will be forwarded through this ISP's connection.
2. If you want to configure and use an APClient Internet connection, please choose **APClient Mode** as the **Operation Mode** in the **Wireless > Basic** page.

5.1.2.1 WAN1 /APClient Internet Connection Settings

For the WAN1 or APClient Internet connection, there are three connection types which include PPPoE, Static IP and DHCP. The following subsections describe how to configure the PPPoE, Static IP and DHCP Internet connection respectively.

5.1.2.1.1 Static IP Internet Connection Settings



The screenshot shows a configuration form for a Static IP Internet Connection. The fields are as follows:

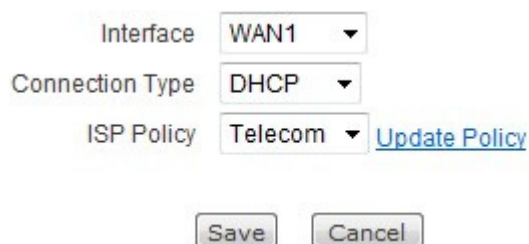
Field	Value
Interface	WAN1
Connection Type	Static IP
ISP Policy	Telecom
IP Address*	200.200.200.52
Subnet Mask*	255.255.255.0
Gateway IP Address*	200.200.200.151
Primary DNS Server*	202.96.199.133
Secondary DNS Server	

Below the form are two buttons: **Save** and **Cancel**. There is also a link labeled [Update Policy](#) next to the ISP Policy dropdown.

Figure 5-6 Static IP Internet Connection

- ◆ **Interface:** It specifies the name of the WAN interface. Here please select **WAN1** or **APClient**.
- ◆ **Connection Type:** It specifies the type of the Internet connection. Here please select **Static IP**. You need to manually configure IP address, subnet mask, default gateway and DNS server addresses, which are provided by your ISP.
- ◆ **ISP Policy:** It specifies the route policy database used for the Internet connection.
- ◆ **Update Policy:** Click to update the corresponding route policy database.
- ◆ **IP Address, Subnet Mask, Default Gateway, Primary DNS Server and Secondary DNS Server:** Refer to **Section 3.3.3.1.1 Static IP Internet Connection Settings** for detailed information.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

5.1.2.1.2 DHCP Internet Connection Settings



The screenshot shows a configuration form for a DHCP Internet Connection. The fields are as follows:

Field	Value
Interface	WAN1
Connection Type	DHCP
ISP Policy	Telecom

Below the form are two buttons: **Save** and **Cancel**. There is also a link labeled [Update Policy](#) next to the ISP Policy dropdown.

Figure 5-7 DHCP Internet Connection Settings

- ◆ **Interface:** It specifies the name of the WAN interface. Here please select **WAN1** or **APClient**.
- ◆ **Connection Type:** It specifies the type of the Internet connection. Here please select **DHCP**. The Gigabit Router will automatically obtain the WAN IP address, subnet mask and gateway and DNS server addresses from your ISP's DHCP server.
- ◆ **ISP Policy** and **Update Policy:** Refer to **Section 5.1.2.1.1 Static IP Internet Connection Settings** for detailed information.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

5.1.2.1.3 PPPoE Internet Connection Settings

Interface: WAN2

Connection Type: PPPoE

ISP Policy: None

User Name*: test

Password*: ••••••

PPP Authentication: Either

Dial Type: Always On

Dial Mode: Normal Mode

Idle Timeout*: 0 Minute

MTU*: 1480 Byte

(MTU Range: 1-1492)

Save Cancel

Figure 5-8 PPPoE Internet Connection Settings

- ◆ **Interface:** It specifies the name of the WAN interface. Here please select **WAN1** or **APClient**.
- ◆ **Connection Type:** It specifies the type of the Internet connection. Here please select **PPPoE**. The Gigabit Router will automatically obtain the WAN IP address, subnet mask and gateway IP address from your ISP's PPPoE server.
- ◆ **ISP Policy** and **Update Policy:** Refer to **Section 5.1.2.1.1 Static IP Internet Connection Settings** for detailed information.
- ◆ **User Name** and **Password:** They specify the PPPoE login user name and password provided by your ISP. Please ask your ISP if you have any questions.
- ◆ **PPP Authentication:** It specifies the PPP authentication mode of the PPPoE

connection. The available options are **Either**, **PAP**, **CHAP** and **NONE**. The default value is **Either**, which means that the Gigabit Router will automatically negotiate it with the remote PPPoE Server. **NONE** means that no authentication is performed.

◆ **Dial Type:** It specifies the dial type of the PPPoE connection. The available options are **Always On**, **Manual** and **On Demand**.

- **Always On:** If you want the Gigabit Router to establish the PPPoE connection when starting up and to automatically re-establish the PPPoE connection once disconnected, please select this option.
- **Manual:** If you want to connect and disconnect the PPPoE connection manually in the **Internet connection List** (see **Section 5.1.1.3 How to Connect and Disconnect a PPPoE/3G Connection**), please select this option.
- **On Demand:** If you want the Gigabit Router to establish the PPPoE connection only when it listens for packets destined for the Internet, please select this option.

◆ **Dial Mode:** It specifies the dial mode of the PPPoE Internet connection. The default value is **Normal mode**. If the PPPoE connection isn't established successfully even using correct user name and password, you may try to use another mode.

◆ **Idle Timeout:** It specifies how long the PPPoE connection keeps connected since no Internet activity. The Gigabit Router will automatically terminate the connection after it has been inactive for the specified period of time. The default value is zero, which means that the Gigabit Router will not terminate it.

◆ **MTU:** It the maximum packet size that can be transmitted over a network. When dialing, the Gigabit Router will automatically negotiate it with the peer device. Please leave the default value of 1480 bytes, unless you have a special application.

▶ **Save:** Click to save your changes.

▶ **Cancel:** Click to revert to the last saved settings.

5.1.2.2 3G Internet Connection Settings

To configure a 3G Internet connection, select **3G** from the Interface drop-down list. Then the following page will be shown.

Interface	3G
ISP Policy	None
3G USB Modem	HUAWEI E169
ISP	China Mobile
Authentication Method	SIM
PIN Code	
APN	CMNET
Dial Number	*99***1#
Advanced PPP Settings:	
User Name	CMNET
Password	•••••

Note: Please follow your ISP's instructions to enter the correct parameters, next click "Save". Then the Router will start to dial. It may take a minute or so, depending on the model of your 3G USB modem. Please click "Refresh" to view the 3G connection status. If it fails to dial, please try to pull out and insert the 3G USB modem again or restart the Router.

Save Cancel

Figure 5-9 3G Internet Connection Settings

- ◆ **Interface:** It specifies the name of the WAN interface. Here please select **3G**.
- ◆ **ISP Policy** and **Update Policy:** Refer to **Section 5.1.2.1.1 Static IP Internet Connection** for detailed information.
- ◆ **3G USB Modem, ISP, Authentication Method, PIN Code, APN, Dial Number, User Name, and Password:** Refer to **Section 3.3.3.2 3G Internet Connection Settings** for detailed information.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.



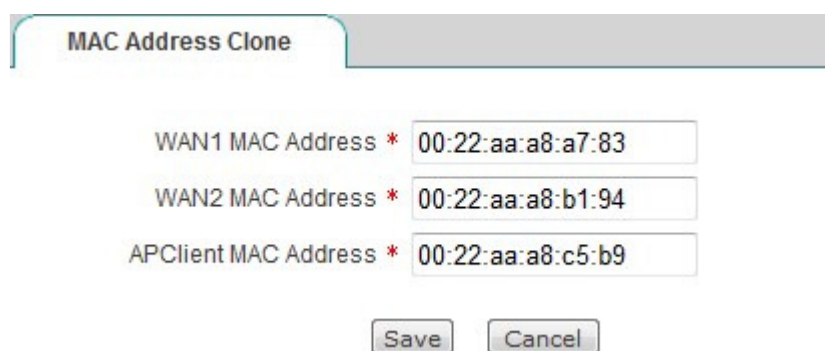
Note

It is strongly recommended that you configure only the **3G USB Modem** and **ISP** of the 3G Internet connection, and leave the other parameters at their default values. If necessary, please follow your ISP's instructions to change them. After you click the **Save** button, the Gigabit Router will start to dial. It may take a minute or so, depending on the model of your 3G USB modem. Please click the **Refresh** button to view the 3G connection status. If it fails to dial, please try to pull out and insert the 3G USB modem again or restart the Gigabit Router.

5.1.3 MAC Address Clone

Some ISPs register the MAC address of your network device (usually a computer) when your account is first opened, and they will only accept traffic from that MAC address. With MAC address clone feature, you may assign the registered MAC address to the Gigabit Router's external interface if you don't want to re-register the MAC address with your ISP.

To configure MAC address clone, go to the **Network > WAN** page, and then select the **MAC Address Clone** tab to go to the setup page shown in Figure 5-10 MAC Address Clone. In this page, you can change the MAC address of each external interface (WAN1 or APClient interface) as required.



MAC Address Clone

WAN1 MAC Address * 00:22:aa:a8:a7:83

WAN2 MAC Address * 00:22:aa:a8:b1:94

APClient MAC Address * 00:22:aa:a8:c5:b9

Save Cancel

Figure 5-10 MAC Address Clone

- ◆ **WAN1 MAC Address:** It specifies the MAC address of the Gigabit Router's WAN1 interface.
- ◆ **APClient MAC Address:** It specifies the MAC address of the Gigabit Router's APClient interface.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

5.2 Load Balancing

This section describes the **Network > Load Balancing** page.

In this page, you can configure load balancing global parameters, the connection detection parameters (including detection target IP, detection interval, retry times, etc.) for each Internet connection, and view the status and configuration of them.

5.2.1 Introduction to Load Balancing and Failover

5.2.1.1 Internet Connection Detection Mechanism

When using multiple Internet connections, to ensure that the network will not be interrupted when a connection is faulty, the Gigabit Router should have the ability of real-time monitoring each Internet connection. To this end, we design flexible automatic detection mechanism on the Gigabit Router, and provide multiple detection methods to meet the actual requirements.

For the sake of convenience, we firstly introduce several related parameters including **Detection Target IP**, **Detection Interval**, **Retry Times**, and **Detection Period**.

- **Detection Target IP:** It indicates the IP address of a target device. The Gigabit Router will monitor an Internet connection by sending detection packets to the specified target IP address.
- **Detection Interval:** It indicates the time interval at which the Gigabit Router periodically sends detection packets, one packet at a time. The default value is 0, which means that connection detection is disabled.
- **Retry Times:** It indicates the number of retries per detection period.
- **Detection Period:** It indicates a period of time during which the Gigabit Router detects whether the Internet connection is available or not. Its value is the product of **Detection Interval** and **Retry Times**. For example, if the **Detection Interval** is set to 10 seconds and the **Retry Times** is set to 3, then the **Detection Period** is 30 ($10 \times 3 = 30$) seconds.

For a normal Internet connection and a faulty Internet connection, the detection mechanisms are different, the following describes them respectively.

For a normal Internet connection, the detection mechanism is as follows: The Gigabit Router periodically sends a detection packet at the specified time interval to the target IP address. Once no response packet received during a detection period, the Gigabit Router will consider that the connection is faulty and shield it immediately. For example, when the **Retry Times** is set to 5, if the Gigabit Router has sent five consecutive detection packets

but not received any response packet during a detection period, it will consider that the connection is faulty.

For a faulty Internet connection, the detection mechanism is as follows: Similarly, the Gigabit Router also periodically sends a detection packet at the specified time interval to the target IP address. Once more than half of the response packets received during a detection period, the Gigabit Router will consider that the connection is back to normal and enable it immediately. For example, when the **Retry Times** is set to 5, if the Gigabit Router has sent five consecutive detection packets and received three or more packets during a detection period, it will consider that the connection is back to normal.

On the Gigabit Router, you can assign a preferential Internet connection to some local computers in advance by setting the connection's **Start Internal IP** and **End Internal IP**, thus the computers in the specified address range will preferentially use the assigned Internet connection to access the Internet. If the assigned Internet connection is normal, those computers can only use it to access the Internet. Else, they will use other normal Internet connections to access the Internet.

**Note**

If you don't want to monitor an Internet connection, please leave its **Detection Interval** at the default value of 0.

5.2.1.2 Load Balancing Mode

The Gigabit Router provides two connection groups: primary connection group and backup connection group. An Internet connection in the primary connection group is a primary connection, while an Internet connection in the backup connection group is a backup connection. By default, all the Internet connections are primary connections. You can move one or more connections into the backup connection group if needed.

The Gigabit Router provides two load balancing modes: **Full Load Balancing** and **Partial Load Balancing**.

If you choose to use **Full Load Balancing**, all the Internet connections are used as primary connections. The working principle is as follows:

1. If all the Internet connections are normal, the LAN users will use these connections to access the Internet.
2. If an Internet connection is faulty, the Gigabit Router will shield it immediately, and the traffic through the faulty connection will be distributed to other normal connections automatically.
3. Once the faulty connection is back to normal, the Gigabit Router will enable it immediately, and the traffic will be redistributed automatically.

If you choose to use **Partial Load Balancing**, some Internet connections are used as

primary connections, and others are used as backup connections. The working principle is as follows:

1. As long as one or more primary connections are normal, the LAN users will use the primary connection(s) to access the Internet.
2. If all the primary connections are faulty, it will automatically switch to the backup connection(s) to let the LAN users use them to access the Internet.
3. Once one or more faulty primary connections are back to normal, it will automatically switch back to the primary connection.

**Note**

During connections switching, some user applications (such as some online games) may be interrupted unexpectedly due to the nature of TCP connection.

5.2.2 Load Balancing Global Settings

The following sections describe the global settings related to **Full Load Balancing** and **Partial Load Balancing** respectively. For more information, please refer to **Section 5.2.1.2 Load Balancing Mode**.

5.2.2.1 Global Settings - Full Load Balancing

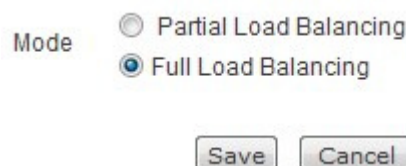


Figure 5-11 Global Settings - Full Load Balancing

◆ **Mode:** It specifies the mode of load balancing. Here please leave the default value of **Full Load Balancing**.

▶ **Save:** Click to save your changes.

▶ **Cancel:** Click to revert to the last saved settings.

5.2.2.2 Global Settings - Partial Load Balancing

Mode ☒ Partial Load Balancing
☐ Full Load Balancing

Primary

WAN1
3G

==>

<==

Backup

APClient
WAN2

Figure 5-12 Global Settings - Partial Load Balancing

- ◆ **Mode:** It specifies the mode of load balancing. Here please select **Partial Load Balancing**.
- ◆ **Primary:** It specifies the primary connection group. An Internet connection in the **Primary** list box is a primary connection.
- ◆ **Backup:** It specifies the backup connection group. An Internet connection in the **Backup** list box is a backup connection.
- ▶ **==>:** Select one or more Internet connections in the **Primary** list box, and then click ==> to move the selected connection(s) to the **Backup** list box.
- ▶ **<==:** Select one or more Internet connections in the **Backup** list box, and then click <== to move the selected connection(s) to the **Primary** list box.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

5.2.3 Load Balancing List

Load Balancing List								4/4
1/1	First	Prev	Next	Last	Go to Page		Search	
Interface	Connection Type	Bandwidth	Status	IP Address	Detection Interval	Retry Times	Detection Target	
WAN1	PPPoE	512k bit/s	Connected	114.62.6.11	0	10	1.1.1.1	
WAN2	DHCP	512k bit/s	Disconnected		0	10	1.1.1.1	
3G	PPPoE	512k bit/s	Disconnected		0	10		
APClient	None							

Figure 5-13 Load Balancing List

Load Balancing List								4/4
1/1	First	Prev	Next	Last	Go to Page		Search	
Status	IP Address	Detection Interval	Retry Times	Detection Target IP	Internal IP Start	Internal IP End	Edit	
Connected	114.62.6.11	0	10	1.1.1.1				
Disconnected		0	10	1.1.1.1				
Disconnected		0	10					
								

Figure 5-14 Load Balancing List (Continue)

- **Edit an Internet Connection:** To configure or modify the detection related parameters of an Internet connection, click its **Interface** hyperlink or  icon, the related information will be displayed in the **Connection Detection Settings** page. Then configure or modify it, and click the **Save** button.
- **View Load Balancing List:** When you have configured load balancing global settings and connection detection settings, you can view the related configuration and status in the **Load Balancing List**.
- **Refresh Load Balancing List:** Click the **Refresh** button to view the latest information in the list.

5.2.4 Connection Detection Settings

You can configure the connection detection related parameters for each Internet connection as required. The operation is as follows: Go to the **Network > Load Balancing > Load Balancing List** page, and click an Internet connection's **Interface** hyperlink or  icon to go the **Connection Detection Settings** page to configure them.

Interface: WAN1

Detection Interval * 0 Sec
(Range: 1-60; 0: Detection is disabled.)

Retry Times * 10 (Range: 3-1000)

Detection Target IP * 1.1.1.1

Bandwidth * 512 kbit/s <== 512K

Start Internal IP

End Internal IP

Save Cancel Back

Figure 5-15 Connection Detection Settings

- ◆ **Interface:** It indicates the name of the WAN interface. It is non-editable.
- ◆ **Detection Interval:** It specifies the time interval at which the Gigabit Router periodically sends detection packets, one packet at a time. It must be between 1 and 60 seconds, or 0. The default value is 0, which means that connection detection is disabled on the Internet connection.
- ◆ **Retry Times:** It specifies the number of retries per detection period. The default value is 3.
- ◆ **Detection Target IP:** It specifies the IP address of a detection target device. The Gigabit Router will monitor the Internet connection by sending the detection packets to the detection target IP address.
- ◆ **Bandwidth:** It specifies the Internet connection's bandwidth, which is provided by your ISP.
- ◆ **Start Internal IP and End Internal IP:** They specify a range of internal IP addresses. The local computers within the specified range will preferentially use the Internet connection. Refer to **Section 5.2.1.1 Internet Connection Detection Mechanism** for more information.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Load Balancing List** page.



Note

The **Detection Target IP**, **Detection Interval**, and **Retry Times** are connection detection related parameters. Please refer to **Section 5.2.1.1 Internet Connection Detection Mechanism** for more information.

5.2.5 How to Configure Connection Detection Settings

To configure connection detection settings, follow these steps:

- Step 1** Go to the **Network > Load Balancing > Load Balancing List** page.
- Step 2** Click an Internet connection's **Interface** hyperlink or  icon to go the **Connection Detection Settings** page.
- Step 3** Configure detection related parameters (**Detection Target IP**, **Detection Interval**, **Retry Times**, etc.) for the selected Internet connection as required.
- Step 4** Click the **Save** button to save your changes.
- Step 5** To configure the detection settings for another Internet connection, please repeat the above steps.

5.3 LAN Settings

This section describes the **Network > LAN** page, where you can configure the IP address, subnet mask and MAC address of the Gigabit Router's LAN interface.

The screenshot shows a web interface for configuring the LAN interface. It contains three input fields: 'IP Address *' with the value '192.168.1.1', 'Subnet Mask *' with the value '255.255.255.0', and 'MAC Address *' with the value '00:22:AA:A8:9D:73'. Below these fields is a note: 'Note: If you change the IP address, you must use the new IP address to re-login to the Router.' At the bottom are two buttons: 'Save' and 'Cancel'.

Figure 5-16 LAN Interface Settings

- ◆ **IP Address:** It specifies the IP address of the LAN interface.
- ◆ **Subnet Mask:** It specifies the subnet mask that defines the range of the LAN.
- ◆ **MAC Address:** It specifies the MAC address of the LAN interface. In most cases, please leave the default value.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.



Note

If you have changed the IP address of the LAN interface and saved the change, you must use the new IP address to re-login to the Gigabit Router.

5.4 DHCP Server

This section describes the **Network > DHCP Server** page, which includes DHCP server settings, static DHCP and DHCP client list.

5.4.1 DHCP Server Settings

Enable DHCP Server ☒

To make the DHCP server related settings take effect, select the check box to enable DHCP server.

Start IP Address * 192.168.1.100

End IP Address * 192.168.1.200

Subnet Mask * 255.255.255.0

Gateway IP Address * 192.168.1.1

Lease Time * 86400 Second

Primary DNS Server * 192.168.1.1

Secondary DNS Server

Enable DNS Proxy ☒

To make the DNS Proxy related settings take effect, select the check box to enable DNS Proxy.

ISP DNS Server 1

ISP DNS Server 2

The ISP DNS servers have higher priority than the primary and backup DNS servers.

Save Cancel

Figure 5-17 DHCP Server Settings

- ◆ **Enable DHCP Server:** It allows you to enable or disable DHCP server. If you want to enable DHCP server on the Gigabit Router, please select this check box.
- ◆ **Start IP Address:** It specifies the first IP address assigned by the DHCP server. In most cases, this address must be on the same subnet as the Gigabit Router's LAN IP address.
- ◆ **End IP Address:** It specifies the last IP address assigned by the DHCP server. In

most cases, this address must be on the same subnet as the Gigabit Router's LAN IP address.

- ◆ **Subnet Mask:** It specifies the subnet mask of the IP addresses assigned by the DHCP server. In most cases, this subnet mask must be identical to the Gigabit Router's LAN subnet mask.
- ◆ **Default Gateway:** It specifies the IP address of the default gateway for a DHCP client. In most cases, this address must be identical to the Gigabit Router's LAN IP address, that is, the Gigabit Router is used as the default gateway for the local computers.
- ◆ **Lease Time:** It specifies the length of time (in seconds) during which a DHCP client can use an assigned IP address.
- ◆ **Primary DNS Server:** It specifies the IP address of the primary DNS server that is available to a DHCP client.
- ◆ **Secondary DNS Server:** It specifies the IP address of the secondary DNS server that is available to a DHCP client.
- ◆ **Enable DNS Proxy:** It allows you to enable or disable DNS proxy. If you want to enable DNS proxy on the Gigabit Router, please select this check box. When acting as a DNS proxy, the Gigabit Router listens for incoming DNS requests on the LAN interface, relays the DNS requests to the current public DNS servers, and replies as a DNS resolver to the requesting local computers.
- ◆ **ISP DNS Server 1 and ISP DNS Server 2:** They specify the IP addresses of the ISP DNS servers.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.



Note

1. If you want a local computer to obtain an IP address and other TCP/IP parameters from the Gigabit Router's built-in DHCP server, please configure the computer to obtain an IP address automatically.
2. If the DNS proxy is enabled on the Gigabit Router, in order to use DNS proxy service normally, you need to set the local computers' primary DNS server to the Gigabit Router's LAN IP address. In addition, if the DHCP server is also enabled on the Gigabit Router, the Gigabit Router will assign its LAN IP address as the primary DNS server address to the local computers automatically.
3. To ensure that the DNS proxy works well, you must at least specify the primary DNS server provided by your ISP on the Gigabit Router.
4. The Gigabit Router can act as a DNS proxy server to all local computers. This greatly simplifies configuration of your local computers. For example, there is a LAN DNS proxy server on which a DNS proxy software is installed (e.g., Wingate), and the local

computers use this server as the primary DNS server. Now, the Gigabit Router will be used as a new gateway for the local computers. In this case, in order to use DNS proxy service normally, the administrator only need to change the Gigabit Router's LAN IP address to the old proxy DNS server's IP address, and enable DNS proxy on the Gigabit Router, without having to change each computer.

5.4.2 Static DHCP

The Gigabit Router offers static DHCP feature which allows you to manually bind an IP address to a computer's MAC address and thus that computer will always obtain the same IP address from the DHCP server. More specifically, each time the specified computer boots and requests its IP address from the Gigabit Router's DHCP server, the DHCP server will recognize the computer's MAC address and always assign the reserved IP address to it.

5.4.2.1 Static DHCP Settings

User Name * test1

IP Address * 192.168.1.150

MAC Address * 0022aa112233

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Save Cancel Back

Figure 5-18 Static DHCP Settings

- ◆ **User Name:** It specifies a unique user name of the DHCP client that wants to be assigned a static IP address.
- ◆ **IP Address:** It specifies the IP address that you want to reserve for the DHCP client. It must be a valid IP address within the range of IP addresses assigned by the DHCP server.
- ◆ **MAC Address:** It specifies the MAC address of the DHCP client.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Network > DHCP Server > Static DHCP** page.

**Note**

1. The reserved IP address must be a valid IP address within the range of IP addresses assigned by the DHCP server.
2. After you have added the static DHCP entry successfully, the Gigabit Router will always assign the reserved IP address to the specified computer.

5.4.2.2 Static DHCP List

Static DHCP List					2/50	
1/1	First	Prev	Next	Last	Go to Page	Search
	User Name	IP Address	MAC Address	Edit		
☐	test1	192.168.1.150	00:22:AA:11:22:33	 		
☐	test2	192.168.1.151	00:22:AA:22:33:44	 		
☐						
☐						
☐						

☐ Select All
 Add
Delete All
Delete

Figure 5-19 Static DHCP List

- **Add a Static DHCP Entry:** To add a new static DHCP entry, first click the **Add** button to go to the **Static DHCP Settings** page, next configure it, lastly click the **Save** button.
- **View Static DHCP Entry(s):** When you have configured one or more static DHCP entries, you can view them in the **Static DHCP List**.
- **Modify a Static DHCP Entry:** To modify a configured static DHCP entry, click its **User Name** hyperlink or  icon, the related information will be displayed in the **Static DHCP Settings** page. Then modify it, and click the **Save** button.
- **Delete Static DHCP Entry(s):** There are three ways to delete static DHCP entry(s).
 1. To delete a static DHCP entry, directly click its  icon.
 2. To delete more than one static DHCP entry at a time, select the leftmost check boxes of the static DHCP entries that you want to delete, and then click the **Delete** button.
 3. To delete all the static DHCP entries at a time, directly click the **Delete All** button.

5.4.2.3 How to Add Static DHCP Entries

To add one or more static DHCP entries, follow these steps:

- Step 1** Go to the **Network > DHCP Server > Static DHCP** page.
- Step 2** Click the **Add** button to go to the **Static DHCP Settings** page, and then specify the **User Name**, **IP Address** and **MAC Address**, lastly click the **Save** button.
- Step 3** Now you can view the static DHCP entry in the **Static DHCP List**.
- Step 4** To add another static DHCP entry, please repeat the above steps.



Note

If you want to delete static DHCP entry(s), please follow the ways described in **Section 5.4.2.2 Static DHCP List**.

5.4.3 DHCP Client List

DHCP Client List

1/1

1/1

First

Prev

Next

Last

Go to

Page

Search

IP Address	Subnet Mask	MAC Address	Lease Left
192.168.1.100	255.255.255.0	60:EB:69:96:9B:6E	86400 Second

Refresh

Figure 5-20 DHCP Client List

- ◆ **IP Address:** It displays the IP address assigned to the DHCP client.
- ◆ **Subnet Mask:** It displays the subnet mask of the current IP address.
- ◆ **MAC Address:** It displays the MAC address of the DHCP client.
- ◆ **Lease Left:** It displays the time remaining (in seconds) until the current IP address lease expires.

▶ **Refresh:** Click to view the latest information in the list.



Note

The **DHCP Client List** only displays the DHCP clients with dynamically assigned IP addresses. It doesn't display the DHCP clients specified by the static DHCP entries.

5.4.4 Configuration Example for DHCP

1. Requirements

In this example, the Gigabit Router acts as a DHCP server to dynamically assign the IP addresses to the clients that reside on the same subnet. The Gigabit Router's LAN IP address is 192.168.1.1/24. The start IP address of the DHCP address pool is 192.168.1.11, and the number of addresses is 100.

Besides, there are two computers that must always have the same IP address: one's MAC address is 00:21:85:9B:45:46 and IP address is 192.168.1.15, the other's MAC address is 00:1f:3c:0f:07:f4 and IP address is 192.168.1.16.

2. Configuration Steps

Step 1 Go to the **Network > DHCP Server > DHCP Server Settings** page.

Step 2 As shown in the following figure, select the **Enable DHCP Server** check box, and enter **192.168.1.11** and **192.168.1.110** in the **Start IP Address** and **End IP Address** text boxes respectively. Leave the other parameters at their default values. Then click the **Save** button to save the settings.

Enable DHCP Server ☒

To make the DHCP server related settings take effect, select the check box to enable DHCP server.

Start IP Address *

End IP Address *

Subnet Mask *

Gateway IP Address *

Lease Time * Second

Primary DNS Server *

Secondary DNS Server

Enable DNS Proxy ☒

To make the DNS Proxy related settings take effect, select the check box to enable DNS Proxy.

ISP DNS Server 1

ISP DNS Server 2

The ISP DNS servers have higher priority than the primary and backup DNS servers.

Figure 5-21 DHCP Server Settings - Example

Step 3 Go to the **Network > DHCP Server > Static DHCP** page.

Step 4 Add the static DHCP entry 1: Click the **Add** button to go to the **Static DHCP Settings** page (see Figure 5-22), enter **Server1** in the **User Name** text box, **192.168.1.15** in the **IP Address** text box, and **0021859B4546** in the **MAC Address** text box, and then click the **Save** button.

User Name *

IP Address *

MAC Address *

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Figure 5-22 Adding the Static DHCP Entry 1 - Example

Step 5 Add the static DHCP entry 2: Click the **Add** button to go to the **Static DHCP Settings** page (see Figure 5-23), enter **Server2** in the **User Name** text box,

192.168.1.16 in the **IP Address** text box, and **001f3c0f07f4** in the **MAC Address** text box, and then click the **Save** button.

User Name *

IP Address *

MAC Address *

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Figure 5-23 Adding the Static DHCP Entry 2 - Example

Now you have configured the two static DHCP entries. You can view them in the **Static DHCP List** (see Figure 5-24), and you can directly click the  icon to modify either of them if desired.

Static DHCP List 2/50

1/1FirstPrevNextLastGo to PageSearch

	User Name	IP Address	MAC Address	Edit
☐	Server1	192.168.1.15	00:21:85:9B:45:46	 
☐	Server2	192.168.1.16	00:1F:3C:0F:07:F4	 

☐ Select All

AddDelete AllDelete

Figure 5-24 Static DHCP List - Example

5.5 DDNS

This section describes the **Network > DDNS** page. In this page, you can not only configure DDNS parameters, but also view and update DDNS status.

5.5.1 Introduction to DDNS

Dynamic Domain Name Service (DDNS) is a service used to map a domain name which never changes to a dynamic IP address which can change quite often. For example, if you have applied for a PPPoE connection with a dynamically assigned IP address from the ISP's PPPoE server, you can use DDNS to allow the external computers to access the Gigabit Router by a constant domain name.

In order to use DDNS service, you should apply for a DDNS account from a DDNS service provider. Each DDNS provider offers its own specific network services. The DDNS service provider reserves the right to change, suspend or terminate your use of some or all network services at any time for any reason. The DDNS service providers supported by UTT Technologies Co., Ltd. currently provide free DDNS services, but they may charge for the DDNS services in the future. In this case, UTT Technologies Co., Ltd. will notify you as soon as possible; if you refuse to pay for the services, you will no longer be able to use them. During the free phase, UTT Technologies Co., Ltd. does not guarantee that the DDNS services can meet your requirements and will be uninterrupted, and UTT does not guarantee the timeliness, security and accuracy of the services.

So far, UTT Technologies Co., Ltd. supports only two DDNS service providers: iplink.com.cn and 3322.org. It will successively support other DDNS service providers in the future.

5.5.2 Apply for a DDNS Account

Please login to <http://www.3322.org> or <http://www.utt.com.cn/ddns> to apply for a fully qualified domain name (FQDN). This section describes how to apply for a FQDN with suffix of 3322.org from <http://www.3322.org>.



主机名: avery12345 . 3322.org ▼
什么是主机名?

泛域名: ☐ 什么是泛域名?

IP 地址: 58.246.187.126

☐ 我有邮件服务器 什么是邮件服务器?

创建动态域名

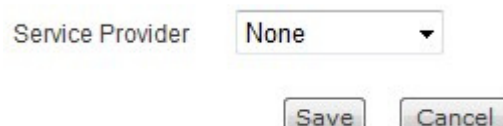
Figure 5-25 Apply for a DDNS Account from 3322.org

- ◆ **Host Name:** It specifies a unique host name of the Gigabit Router. The suffix of 3322.org will be appended to the host name to create a fully qualified domain name (FQDN) for the Gigabit Router. For example, if the Gigabit Router's host name is **test**, then its FQDN is **test.3322.org**; and it allows you to use **test.3322.org** to access the Gigabit Router.
- ◆ **IP Address:** It specifies the IP address mapped to the registered domain name of the Gigabit Router.
- ▶ **Register:** Click to register the domain name.

5.5.3 DDNS Settings

5.5.3.1 Disabling DDNS Service

If you want to disable DDNS service, please leave the **Service Provider** at its default value of **None**, see Figure 5-26.



Service Provider None ▼

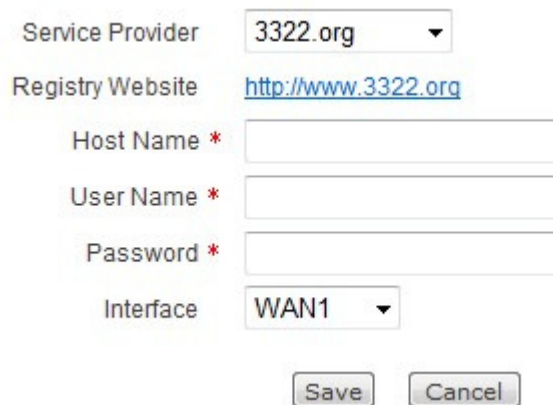
Save Cancel

Figure 5-26 Disabling DDNS Service

- ◆ **Service Provider:** It specifies the DDNS service provider who offers services to the Gigabit Router. Here please select **None** to disable DDNS service.
- ▶ **Save:** Click to save your changes.

- ▶ **Cancel:** Click to revert to the last saved settings.

5.5.3.2 DDNS Service Offered by 3322.org



The screenshot shows a web form for configuring DDNS settings. The 'Service Provider' is set to '3322.org'. The 'Registry Website' is a clickable link to 'http://www.3322.org'. There are three input fields for 'Host Name', 'User Name', and 'Password', each marked with a red asterisk. The 'Interface' is set to 'WAN1'. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 5-27 DDNS Settings Related to 3322.org

- ◆ **Service Provider:** It specifies the DDNS service provider who offers services to the Gigabit Router. Now the Gigabit Router only supports two DDNS service providers: **iplink.com.cn** and **3322.org**. Here please select **3322.org**.
- ◆ **Registry Website:** It allows you to click <http://www.3322.org> to go to this website to register a DDNS account for the Gigabit Router.
- ◆ **Host Name:** It specifies the host name of the Gigabit Router. It must be identical to the host name that you entered when registering the DDNS account on the website <http://www.3322.org>.
- ◆ **User Name:** It specifies the user name that you entered when registering your user account on the website <http://www.3322.org>.
- ◆ **Password:** It specifies the password that you entered when registering your user account on the website <http://www.3322.org>.
- ◆ **Interface:** It specifies the interface on which DDNS service is applied.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

5.5.3.3 DDNS Service Offered by IPLink

Service Provider:

Registry Website: <http://www.utt.com.cn/ddns>
Registration Number: 11050355

Host Name *:

Key *:

Interface:

If the service provider is iplink.com.cn, you should choose **Synchronize with SNTP Server in System > Time.**

Figure 5-28 DDNS Settings Related to iplink.com.cn

- ◆ **Service Provider:** It specifies the DDNS service provider who offers services to the Gigabit Router. Now the Gigabit Router only supports two DDNS service providers: **iplink.com.cn** and **3322.org**. Here please select **iplink.com.cn**.
- ◆ **Registry Website:** It allows you to click <http://www.utt.com.cn/ddns> to go to this website to register a DDNS account for the Gigabit Router.
- ◆ **Registration Number:** It specifies the registration number of the Gigabit Router.
- ◆ **Host Name:** It specifies the host name of the Gigabit Router. It must be identical to the host name that you entered when registering the DDNS account on the website <http://www.utt.com.cn/ddns>.
- ◆ **Key:** It specifies the key that you got when registering the DDNS account on the website <http://www.utt.com.cn/ddns>.
- ◆ **Interface:** It specifies the interface on which DDNS service is applied.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

5.5.4 DDNS Status

DDNS Status

Status	Host Name	IP Address	Update Time
Failed	520w1220.iplink.com.cn		

Figure 5-29 DDNS Status

- **Update:** Click to update DDNS status.

5.5.5 DDNS Verification

To verify whether DDNS is updated successfully, you can use the ping command at the command prompt on the PC, for example: **ping avery12345.3322.org**

If the displayed page is similar to the screenshot below: the domain name is resolved to an IP address successfully (58.246.187.126 in this example), DDNS is updated successfully.

```
Pinging avery12345.3322.org [58.246.187.126] with 32 bytes of data:
```

```
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
```

```
Ping statistics for 58.246.187.126:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```



Note

1. Only when the WAN interface IP address is a public IP address, the Internet users can use its mapped domain name to access the Gigabit Router normally.
2. DDNS feature can help you implement VPN tunnels using dynamic IP addresses on the Gigabit Router.

5.6 UPnP

This section describes the **Network > UPnP** page.

The Universal Plug and Play (UPnP) is architecture that implements zero configuration networking, that is, it provides automatic IP configuration and dynamic discovery of the UPnP compatible devices from various vendors. A UPnP compatible device can dynamically join a network and work properly.

When you enable UPnP, the Gigabit Router allows any local UPnP-enabled device to perform a variety of actions, including retrieving the public IP address, enumerating existing port mappings, and adding or removing port mappings. By adding a port mapping, a UPnP-enabled device opens the related service ports on the Gigabit Router to allow outside computers to access.

5.6.1 Enable UPnP



Figure 5-30 Enable UPnP

◆ **Enable UPnP:** It allows you to enable or disable UPnP. If you want to enable UPnP, please select this check box.

▶ **Save:** Click to save your changes.

5.6.2 UPnP Port Forwarding List

The **UPnP Port Forwarding List** lists all the port forwarding entries established using UPnP, see the following figure.

[illegible]

Figure 5-31 UPnP Port Forwarding List

- ◆ **ID:** It is used to identify each UPnP port forwarding entry in the list.
- ◆ **Internal IP:** It displays the IP address of the local computer.
- ◆ **Internal Port:** It displays the service port provided by the local computer.
- ◆ **Protocol:** It displays the transport protocol used by the service.
- ◆ **Remote IP:** It displays the IP address of the remote computer.
- ◆ **External Port:** It displays the external port of the UPnP port forwarding, which is opened for outside user to access.
- ◆ **Description:** It displays the description of the UPnP port forwarding entry.
- ▶ **Refresh:** Click to view the latest information in the list.

Chapter 6 Advanced

This chapter describes how to configure and use the advanced features of the Gigabit Router, which include NAT and DMZ, IP/MAC binding, static route, and PPPoE server.

6.1 NAT and DMZ

This section describes the **Advanced > NAT&DMZ** page.

6.1.1 Introduction to NAT Features

6.1.1.1 NAT Overview

The NAT (Network Address Translation) is an Internet standard that is used to map one IP address space (i.e., Intranet) to another IP address space (i.e., Internet). The NAT is designed to alleviate the shortage of IP addresses, that is, it allows all the local computers to share a single or a small group of IP addresses: On the Internet, there is only a single network device using a single or a small group of public IP addresses; but the local computers can use any range of private IP addresses, and these IP addresses are not visible from the Internet. As the internal network can be effectively isolated from the outside world, the NAT can also provide the benefit of network security assurance.

The Gigabit Router provides flexible NAT features. The following sections describe them in detail.

6.1.1.2 NAT Address Space Definitions

To ensure that NAT operates properly, the Gigabit Router uses and maintains two address spaces:

- **Internal IP address:** It indicates the IP address assigned to a local computer by the administrator. It is usually a private IP address.
- **External IP address:** It indicates the IP address assigned to the Gigabit Router's

Internet connection by the ISP. It is a legal public IP address that can represent one or more internal IP addresses to the outside world.

6.1.1.3 NAT Types

The Gigabit Router provides two types of NAT: **One2One** and **EasyIP**.

- **One2One (One to One):** It indicates static network address translation. It is always referred to as Basic NAT, which provides a one to one mapping between an internal and an external IP address. In this type of NAT, IP address needs to be changed, but port needn't.

One to One NAT can be used to allow the outside users to access a LAN server: In the local network, the LAN server still use the private IP address, which is provided to the local computers to access; and on the Internet, the Gigabit Router will assign an external IP address to the local server, then the outside users can using this external IP address to access the server through the Gigabit Router.

- **EasyIP:** It indicates network address and port translation (NAPT). Since it is the most common type of NAT, it is often simply referred to as NAT. NAPT provides many-to-one mappings between multiple internal IP addresses and a single external IP addresses, that is, these multiple internal IP addresses will be translated to the same external IP address. In this type of NAT, to avoid ambiguity in the handling of returned packets, it must dynamically assign a TCP/UDP port to an outgoing session and change the packets' source port to the assigned port before forwarding them. Besides, the Gigabit Router must maintain a translation table so that return packets can be correctly translated back.

When you obtain multiple public IP addresses from your ISP, you can create more than one NAT rule for either type of NAT. In actual network environment, the two types of NAT rules are often used together.

6.1.1.4 Port Forwarding and DMZ Host

When NAT is enabled on the Gigabit Router, the Gigabit Router will block all the requests initiated from outside users. However, in some cases, the outside users want to access the LAN internal servers through the Gigabit Router. To achieve this purpose, you need to configure port forwarding entries or DMZ host on the Gigabit Router.

1. Port Forwarding

Port forwarding feature allows you to create the mapping between <external IP address: external port> and <internal IP address: internal port>, then all the requests from outside users to the specified external IP address: port on the Gigabit Router will be forwarded to

the mapped local server, so the outside users can access the service offered by the server.

For example, if you want to allow the local SMTP server (IP address: 192.168.1.88) to be available to the outside users, you can create a port forwarding entry: external IP address is WAN1 IP address (200.200.201.88 in this example), external port is 2100, internal IP address is 192.168.1.88, and internal port is 25. Then all the requests to SMTP service from outside users to 200.200.201.88:2100 will be forwarded to 192.168.1.88:25.

2. DMZ Host

The DMZ (Demilitarized Zone) feature allows one local computer to be exposed to the Internet for the use of a special service such as online game or video conferencing. When receiving the requests initiated from outside users, the Gigabit Router will directly forward these requests to the specified DMZ host.



Note

When a local computer is designated as the DMZ host, it loses firewall protection provided by the Gigabit Router. As the DMZ host is exposed to many exploits from the Internet, it may be used to attack your network.

3. The Priorities of Port Forwarding Entries and DMZ Host

The port forwarding entries take priority over the DMZ host. When receiving a request packet initiated from an outside user, the Gigabit Router will firstly search the **Port Forwarding List** to find out if there is a port forwarding entry matching the destination IP address and port of the packet. If a match is found, the Gigabit Router will forward the packet to the mapped local computer. Else, the Gigabit Router will try to find out if there is an available DMZ host.

6.1.2 Port Forwarding

6.1.2.1 Port Forwarding List

Port Forwarding List									1/50
1/1	First	Prev	Next	Last	Go to Page		Search		
	Name	Status	Protocol	Start External Port	Internal IP Address	Start Internal Port	Port Count	Bind to	Edit
☐	admin	Enable	TCP	8081	192.168.1.1	80	1	WAN2	 

☐ Select All

Figure 6-1 Port Forwarding List

- ▶ **Add a Port Forwarding Entry:** To add a new port forwarding entry, first click the **Add** button to go to the **Port Forwarding Settings** page, next configure it, lastly click the **Save** button.
- ▶ **View Port Forwarding Entry(s):** When you have configured one or more port forwarding entries, you can view them in the **Port Forwarding List**.
- ▶ **Modify a Port Forwarding Entry:** To modify a configured port forwarding entry, click its **Name** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete Port Forwarding Entry(s):** There are three ways to delete port forwarding entry(s).
 1. To delete a port forwarding entry, directly click its  icon.
 2. To delete more than one port forwarding entry at a time, select the leftmost check boxes of the entries that you want to delete, and then click the **Delete** button.
 3. To delete all the port forwarding entries at a time, directly click the **Delete All** button.



Note

After you enable HTTP remote management in the **Administration > Remote Access** page, the system will automatically create a port forwarding entry for it. You cannot modify or delete it in this page.

6.1.2.2 Port Forwarding Settings

Name *

Enable ☒

Select the check box to make the port forwarding entry take effect.

Protocol

Start External Port *

IP Address *

The IP address of the local host that provides the service.

Start Internal Port *

Port Count *

Change it if the open service uses a range of consecutive ports.

Bind to

Figure 6-2 Port Forwarding Settings

- ◆ **Name:** It specifies a unique name of the port forwarding entry.
- ◆ **Enable:** It allows you to enable or disable the port forwarding entry. The default value is checked, which means the port forwarding entry is in effect. If you want to disable the entry temporarily instead of deleting it, please clear the check box.
- ◆ **Protocol:** It specifies the transport protocol used by the service. The available options are **TCP**, **UDP** and **TCP/UDP**. If you are not sure, select **TCP/UDP**.
- ◆ **Start External Port:** It specifies the lowest port number provided by the Gigabit Router. The external ports are opened for outside users to access.
- ◆ **Internal IP Address:** It specifies the IP address of the local computer that provides the service.
- ◆ **Start Internal Port:** It specifies the lowest port number of the service provided by the local computer. The **Start External Port** and **Start Internal Port** can be different.
- ◆ **Port Count:** It specifies the number of service ports provided by the local computer. If the service uses only one port number, enter 1. Change it if the service uses a range of consecutive ports. The maximum value is 20. For example, if the start internal port is 20, the start external port is 2000, and the port count is 2, then the internal port range is from 20 to 21, and the external port range is from 2000 to 2001.
- ◆ **Bind to:** It specifies the interface to which this port forwarding entry is bound. The port forwarding entry will use the selected interface's IP address as its external IP address.

- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Port Forwarding List**.

6.1.2.3 How to Add Port Forwarding Entries

To add one or more static port forwarding entries, follow these steps:

- Step 1** Go to the **Advanced > NAT > Port Forwarding** page, and click the **Add** button to go to the **Port Forwarding Settings** page.
- Step 2** Specify the **Name**, and leave the **Enable** check box checked.
- Step 3** Specify the **Protocol**, **Internal IP Address** and **Start Internal Port** as required.
- Step 4** Specify the **Start External Port** as required. The **Start External Port** and **Start Internal Port** can be different.
- Step 5** If the open service uses a range of consecutive ports, you need to specify the **Port Count**.
- Step 6** Select an interface from the **Bind to** drop-down list as required. The port forwarding entry will use the selected interface's IP address as its external IP address.
- Step 7** Click the **Save** button to save the settings. You can view the port forwarding entry in the **Port Forwarding List**.
- Step 8** If you want to add another new port forwarding entry, please repeat the above steps.

6.1.2.4 Configuration Example for Port Forwarding

An organization wants a LAN server (IP Address: 192.168.1.99) to open Web service (Protocol: TCP; Port: 80) to the outside users. And the Gigabit Router will use 10000 as the external port and the WAN1 IP address (200.200.200.88 in this example) as the external IP address. Then all the requests to Web service from outside users to 200.200.200.88:10000 will be forwarded to 192.168.1.99:80.

The following figure shows the detailed settings.

Name *

Enable ☒

Select the check box to make the port forwarding entry take effect.

Protocol

Start External Port *

IP Address *

The IP address of the local host that provides the service.

Start Internal Port *

Port Count *

Change it if the open service uses a range of consecutive ports.

Bind to

Figure 6-3 Port Forwarding Settings - Example

6.1.3 NAT Rule

6.1.3.1 NAT Rule List

NAT Rule List							2/8
1/1	First	Prev	Next	Last	Go to Page		Search
	Name	NAT Type	External IP	Start Internal IP	End Internal IP	Bind to	Edit
☐	Example1	EasyIP	218.1.21.3	192.168.1.10	192.168.1.100	WAN1	 
☐	Example2	One2One	202.1.1.131	192.168.1.200	192.168.1.203	WAN1	 
☐							
☐							
☐							

☐ Select All

Figure 6-4 NAT Rule List

- **Add a NAT Rule:** To add a new NAT rule, first click the **Add** button to go to the **NAT Rule Settings** page, next configure it, lastly click the **Save** button.
- **View NAT Rule(s):** When you have configured one or more NAT rules, you can view them in the **NAT Rule List**.
- **Modify a NAT Rule:** To modify a configured NAT rule, click its **Name** hyperlink or 

icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

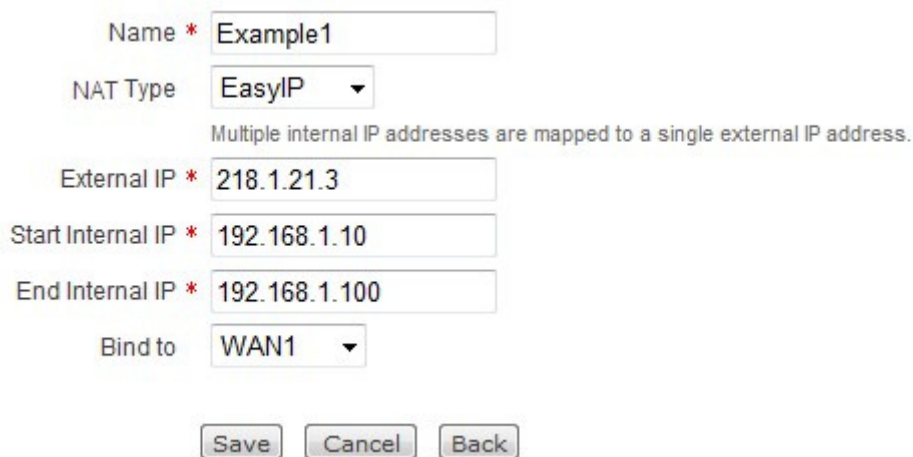
► **Delete NAT Rule(s):** There are three ways to delete NAT rules.

1. To delete a NAT rule, directly click its  icon.
2. To delete more than one NAT rule at a time, select the leftmost check boxes of the NAT rules that you want to delete, and then click the **Delete** button.
3. To delete all the NAT rules at a time, directly click the **Delete All** button.

6.1.3.2 NAT Rule Settings

The following sections describe the settings of the **EasyIP** NAT rule and **One2One** NAT rule respectively, see Figure 6-5 and Figure 6-6.

6.1.3.2.1 NAT Rule Settings - EasyIP



Name *

NAT Type

Multiple internal IP addresses are mapped to a single external IP address.

External IP *

Start Internal IP *

End Internal IP *

Bind to

Figure 6-5 NAT Rule Settings - EasyIP

- ◆ **Name:** It specifies a unique name of the NAT rule.
 - ◆ **NAT Type:** It specifies the type of the NAT rule. The available options are **EasyIP** and **One2One**. Here please select **EasyIP**.
 - ◆ **External IP:** It specifies the external IP address to which the local computers' IP addresses are mapped.
 - ◆ **Start Internal IP** and **End Internal IP:** They specify a range of internal IP addresses. The local computers within the specified range will preferentially use the NAT rule.
 - ◆ **Bind to:** It specifies the interface to which the NAT rule is bound.
- **Save:** Click to save your changes.

- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **NAT Rule List**.

6.1.3.2.2 NAT Rule Settings - One2One



The screenshot shows a web-based configuration form for a NAT rule. The form has the following fields and values:

- Name ***: Example2
- NAT Type**: One2One (dropdown menu)
- Start External IP ***: 202.1.1.131
- Start Internal IP ***: 192.168.1.200
- End Internal IP ***: 192.168.1.203
- Bind to**: WAN1 (dropdown menu)

Below the fields are three buttons: **Save**, **Cancel**, and **Back**. A small text note below the NAT Type dropdown states: "One internal IP address is mapped to one external IP address."

Figure 6-6 NAT Rule Settings - One2One

- ◆ **Name:** It specifies a unique name of the NAT rule.
- ◆ **NAT Type:** It specifies the type of the NAT rule. The available options are **EasyIP** and **One2One**. Here please select **One2One**.
- ◆ **Start External IP:** It specifies the start external IP address to which the start internal IP address is mapped.
- ◆ **Start Internal IP** and **End Internal IP:** They specify the internal IP address range of the NAT rule.
- ◆ **Bind to:** It specifies the interface to which the NAT rule is bound.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **NAT Rule List**.



Note

1. When creating a **One2One** NAT rule, you must set the **Start External IP**. The number of the external IP addresses is the same as the number of internal IP addresses, which is determined by the **Start Internal IP** and **End Internal IP**. For example, if the **Start Internal IP** is 192.168.16.6, **End Internal IP** is 192.168.16.8, and **Start External IP** is 200.200.200.116, then 192.168.16.6, 192.168.16.7, and 192.168.16.8 will be mapped to 200.200.200.116, 200.200.200.117, and 200.200.200.118 respectively.

2. A One2One NAT rule can contain up to 20 external/internal IP addresses.

6.1.3.3 How to Add NAT Rules

To add one or more NAT rules, follow these steps:

- Step 1** Please identify the type of the NAT rule that you want to add.
- Step 2** Go to the **Advanced > NAT > NAT Rule** page, and click the **Add** button to go to the **NAT Rule Settings** page.
- Step 3** Specify the **Name** for the NAT rule, and select a type from the **NAT Type** drop-down list as required.
- Step 4** There are two cases:
- 1) If the NAT rules' type is **EasyIP**, please specify the **External IP**, **Start Internal IP**, and **End Internal IP** as required.
 - 2) If the NAT rules' type is **One2One**, please specify the **Start External IP**, **Start Internal IP**, and **End Internal IP** as required.
- Step 5** Select an interface from the **Bind to** drop-down list as required.
- Step 6** Click the **Save** button to save the settings. You can view the NAT rule in the **NAT Rule List**.
- Step 7** If you want to add another new NAT rule, please repeat the above steps.



Note

If you want to delete NAT rule(s), please follow the ways described in **Section 7.1.3.1 NAT Rule List**.

6.1.3.4 Configuration Examples for NAT Rule

6.1.3.4.1 An Example for Configuring an EasyIP NAT Rule

1. Requirements

In this example, an Internet café has a single Internet connection, and obtains eight public IP addresses (from 218.1.21.0/29 to 218.1.21.7/29) from the ISP. Therein, 218.1.21.1/29 is used as the Internet connection's gateway IP address, 218.1.21.2/29 is used as the Gigabit Router's WAN1 interface IP address. Note that 218.1.21.0/29 and 218.1.21.7/29 cannot be used as they are the subnet number and broadcast address respectively.

The administrator want the local computers in the online game area (its address range is from 192.168.1.10/24 to 192.168.1.100/24) to use 218.1.21.3/29 to access the Internet. To achieve this purpose, he should create an **EasyIP** NAT rule for them. The rule's **External IP** is 218.1.21.3, **Start Internal IP** is 192.168.1.10, **End Internal IP** is 192.168.1.100, and **Bind to** be WAN1.

2. Configuration Steps

The configuration steps are the following:

Step 1 Go to the **Advanced > NAT > NAT Rule** page, and click the **Add** button to go to the **NAT Rule Settings** page, see the following figure.

Name *

NAT Type

Multiple internal IP addresses are mapped to a single external IP address.

External IP *

Start Internal IP *

End Internal IP *

Bind to

Figure 6-7 EasyIP NAT Rule Settings - Example

Step 2 Enter **Example1** in the **Name** text box.

Step 3 Select **EasyIP** from the **NAT Type** drop-down list.

Step 4 Enter **218.1.21.3** in the **External IP** text box; enter **192.168.1.10** and **192.168.1.100** in the **Start Internal IP** and **End Internal IP** text boxes respectively.

Step 5 Select **WAN1** from the **Bind to** drop-down list.

Step 6 Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and you can view it in the **NAT Rule List**.



Note

If an **EasyIP** NAT rule's **External IP** is not on the same subnet as the IP address of the interface to which the rule is bound, the Gigabit Router's default gateway requires a subnet route for the network to which the **External IP** belongs, or a host route for the **External IP** pointing to the bound interface.

6.1.3.4.2 An Example for Configuring a One2One NAT Rule

1. Requirements

In this example, a business has a single static IP Internet connection, and obtains eight public IP addresses (202.1.1.128/29 - 202.1.1.135/29) from the ISP. Therein, 202.1.1.129/29 is used as the Internet connection's gateway IP address, 202.1.1.130/2 is used as the Gigabit Router's WAN1 IP address. Note that 202.1.1.128/29 and 202.1.1.135/29 cannot be used as they are the subnet number and broadcast address respectively.

The business wants its employees to share a single public IP address of 202.1.1.130/29 to access the Internet; and it wants its four local servers to provide services for the outside users. The LAN subnet is 192.168.1.0/24. The four local servers IP addresses are from 192.168.1.200/24 to 192.168.1.203/24.

2. Analysis

Firstly we need to configure a static IP Internet connection on the WAN1 interface in the **Network > WAN** page or through the **Start > Setup Wizard**. After you have configured the Internet connection, the Gigabit Router will automatically create a related system reserved EasyIP NAT rule, and also enable NAT.

Secondly, we need to create a One2One NAT rule for the four local servers. The IP addresses of the four local servers are mapped to 202.1.1.131/29, 202.1.1.132/29, 202.1.1.133/29, 202.1.1.134/29 respectively. Thus the outside users can use these public addresses to access the local servers through the Gigabit Router.

3. Configuration Steps

Here we only describe how to create the **One2One** NAT rule.

Step 1 Go to the **Advanced > NAT > NAT Rule** page, and click the **Add** button to go to the **NAT Rule Settings** page, see the following figure.

Step 2 Enter **Example2** in the **Name** text box.

Name * Example2

NAT Type One2One ▼

One internal IP address is mapped to one external IP address.

Start External IP * 202.1.1.131

Start Internal IP * 192.168.1.200

End Internal IP * 192.168.1.203

Bind to WAN1 ▼

Save Cancel Back

Figure 6-8 One2One NAT Rule Settings - Example

- Step 3** Select **One2One** from the **NAT Type** drop-down list.
- Step 4** Enter **202.1.1.131** in the **Start External IP** text box; enter **192.168.1.200** and **192.168.1.203** in the **Start Internal IP** and **End Internal IP** text boxes respectively.
- Step 5** Select **WAN1** from the **Bind to** drop-down list.
- Step 6** Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and you can view it in the **NAT Rule List**.

6.1.4 DMZ

Enable DMZ ☐

After you enable DMZ, the DMZ host will be exposed to the Internet.

DMZ Host IP Address *

Save Cancel

Figure 6-9 DMZ Host Settings

- ◆ **Enable DMZ:** It allows you to enable or disable DMZ feature. If you want to enable DMZ feature on the Gigabit Router, please select this check box.
- ◆ **DMZ Host IP Address:** It specifies the private IP address of the DMZ host.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

**Note**

When a local computer is designated as the DMZ host, it loses firewall protection provided by the Gigabit Router. The DMZ host can be accessed through all the WAN interfaces.

6.2 IP/MAC Binding

This section describes the **Security > IP/MAC Binding** page.

6.2.1 Introduction to IP/MAC Binding

6.2.1.1 IP/MAC Binding Overview

To achieve network security management, you should perform user identification before performing user authorization. In this section, we describe how to implement user identification. In **Section 9.1 Firewall > Access Control**, we will describe how to control the Internet behaviors of the LAN users in detail.

The Gigabit Router provides IP/MAC binding feature to implement user identification. Using the IP/MAC address pair as a unique user identity, you can protect the Gigabit Router and your network against IP spoofing attacks. IP spoofing attack refers to that a computer attempts to use another trusted computer's IP address to connect to or pass through the Gigabit Router. The computer's IP address can easily be changed to a trusted address, but MAC address cannot easily be changed as it is added to the Ethernet card at the factory.

6.2.1.2 The Operation Principle of IP/MAC Binding

For the sake of convenience, we firstly introduce several related terms including legal user, illegal user and undefined user.

- **Legal User:** A legal user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is checked.
- **Illegal User:** An illegal user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is cleared; or the IP address or MAC address is the same as that of an IP/MAC binding, but not both.
- **Undefined User:** An undefined user's IP address and MAC address both are different from any IP/MAC binding. The undefined users are all the users except legal and illegal users.

It allows the legal users to access the Gigabit Router or access the Internet through the Gigabit Router, and denies the illegal users. And the parameter of **Allow Undefined LAN PCs** determines whether it allows the undefined users to access the Gigabit Router or

access the Internet through the Gigabit Router, that is, it will allow them if they **Allow Undefined LAN PCs** check box is checked, else block them.

IP/MAC binding feature can act on the packets initiated from the local computers to the Gigabit Router or outside computers. When receiving a packet initiated from LAN, the Gigabit Router will firstly determine the sender's identity by comparing the packet with the bindings in the **IP/MAC Binding List**, and then process the packet according to the sender's identity. The details are as follows:

1. If the sender is a legal user, the packet will be allowed to pass, and then be further processed by other function modules.
2. If the sender is an illegal user, the packet will be dropped immediately to prevent IP spoofing.
3. If the sender is an undefined user, there are two cases:
 - 1) If the **Allow Undefined LAN PCs** check box is checked, the packet will be allowed to pass, and then be further processed by other function modules.
 - 2) Else, the packet will be dropped immediately.

6.2.2 IP/MAC Binding Global Settings

Allow Undefined LAN PCs ☒

Figure 6-10 IP/MAC Binding Global Settings

◆ **Allow Undefined LAN PCs:** It allows or blocks the undefined local computers from accessing the Gigabit Router or accessing the Internet through the Gigabit Router. If you want to allow the undefined local computers to access the Gigabit Router and Internet, please select the check box.

► **Save:** Click to save your changes.



Note

If you want to clear the **Allow Undefined LAN PCs** check box to block the undefined local computers, please make sure that you have added the IP/MAC address pair of the computer that you use to administer the Gigabit Router into the **IP/MAC Binding List**. Otherwise you cannot access the Gigabit Router from that computer.

6.2.3 IP/MAC Binding List

IP/MAC Binding List					2/50
1/1	First	Prev	Next	Last	Go to Page
					Search
	User Name	IP Address	MAC Address	Allow	Edit
☐	test1	192.168.1.150	00:22:aa:11:22:33	☒	 
☐	test2	192.168.1.151	00:22:aa:bb:cc:88	☒	 
☐					
☐					
☐					

☐ Select All

Figure 6-11 IP/MAC Binding List

- **Add One or More IP/MAC Bindings:** To add one or more IP/MAC bindings, first click the **Add** button to go to the **IP/MAC Binding Settings** page shown in Figure 6-14, next configure them, lastly click the **Save** button.
- **View IP/MAC Binding(s):** When you have configured one or more IP/MAC bindings, you can view them in the **IP/MAC Binding List**.
- **Modify an IP/MAC Binding:** To modify a configured IP/MAC binding, click its **User Name** hyperlink or  icon, the related information will be displayed in the setup page shown in Figure 6-12. Then modify it, and click the **Save** button.

User Name *

IP Address *

MAC Address *

Figure 6-12 Modifying an IP/MAC Binding

The **Allow** check box is used to allow or block a user matching an IP/MAC binding from accessing the Gigabit Router and Internet. To allow the user matching the IP/MAC binding to access, select the IP/MAC binding's **Allow** check box; else clear it.

- **Delete IP/MAC binding(s):** There are three ways to delete IP/MAC bindings.
 1. To delete a IP/MAC binding, directly click its  icon.
 2. To delete more than one IP/MAC binding at a time, select the leftmost check boxes of the bindings that you want to delete, and then click the **Delete** button.
 3. To delete all the IP/MAC bindings at a time, directly click the **Delete All** button.

**Note**

When you add the IP/MAC address pair of the computer that you use to administer the Gigabit Router into the **IP/MAC Binding List**, please leave the **Allow** check box checked. Otherwise you cannot access the Gigabit Router from that computer. If you attempt to clear the check box, you will be prompted that the operation is not permitted, see the following figure.

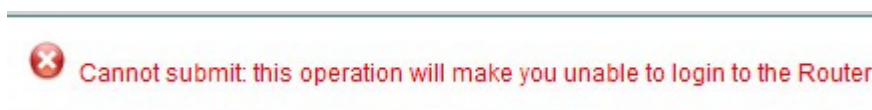


Figure 6-13 IP/MAC Binding Error Message

6.2.4 IP/MAC Binding Settings

1. You can enter one or more IP/MAC binding entries in the text box, which supports edit operations like Cut, Paste, Copy, Delete, etc.
2. The input format of a binding entry is: IP Address MAC Address User Name , e.g., 192.168.1.100 0022aaAFCdb3 Mary
3. There can be one or more spaces between the IP Address and MAC Address, and between the MAC address and User Name.

Figure 6-14 IP/MAC Binding Settings

- ◆ **Subnet:** It specifies the subnet you want to scan. The default is the Gigabit Router's LAN IP address and subnet mask.
- ▶ **Scan:** If you click the **Scan** button, the Gigabit Router will immediately scan the specified subnet to detect active computers connected to the Gigabit Router, learn and display dynamic ARP information (that is, IP and MAC address pairs) in the text

box. Note that if a computer's IP/MAC address pair has been added in the **IP/MAC Binding List**, this IP/MAC address pair will not be displayed here.

- ▶ **Bind:** Click to bind all the valid IP and MAC address pairs in the text box.
- ▶ **Add IP/MAC Binding(s) Manually:** To manually add one or more IP/MAC bindings, follow these steps: Enter one or more IP/MAC address pair entries in the text box, and then click the **Bind** button. The input contents are: **IP Address**, **MAC Address** and **User Name**, one address pair entry per line; and the input format for each entry is: **IP Address <Space> MAC Address <Space> User Name <Enter>**.
 - **IP Address:** It specifies the IP address of the local computer.
 - **MAC Address:** It specifies the MAC address of the local computer.
 - **User Name:** It specifies a unique user name of the local computer whose IP/MAC address pair will be bound. It is an optional parameter. If you don't enter it, the system will automatically create a user name for the computer.



Note

1. You can use the **ipconfig /all** command at the command prompt to find a Windows-based computer's IP address and MAC address.
2. For an IP/MAC address pair entry entered manually, there can be one or more spaces between the **IP Address** and **MAC Address**, and between the **MAC address** and **User Name**.
3. The **Bind** operation will skip any invalid IP and MAC address pairs in the text box. In other words, it will only bind the valid IP and MAC address pairs.

6.2.5 How to Add IP/MAC Bindings

To add one or more IP/MAC bindings, follow these steps:

- Step 1** Go to the **Advanced > IP/MAC Binding** page, and click the **Add** button to go to the **IP/MAC Binding Settings** page.
- Step 2** There are two methods to add IP/MAC bindings:
- 1) **Method One:** Click the **Scan** button to learn current dynamic ARP information (that is, IP and MAC address pairs) of the local computers, next click the **Bind** button to bind the valid IP/MAC address pairs in the text box.
 - 2) **Method Two:** You can manually add one or more IP/MAC address pairs in the text box, next click the **Bind** button to bind these IP/MAC address pairs. Refer to **Section 7.2.4 IP/MAC Binding Settings** for more information.
- Step 3** After you have added some IP/MAC bindings, you can view them in the **IP/MAC**

Binding List.

- Step 4** If you want to block the undefined local computers from accessing the Gigabit Router and Internet, please clear the **Allow Undefined LAN PCs** check box; else, the undefined local computers are allowed to access the Gigabit Router and Internet.
- Step 5** If you want to temporarily block a user matching an IP/MAC binding from accessing the Gigabit Router and Internet, please clear the binding's **Allow** check box.

After you have finished configuring IP/MAC binding feature, when receiving a packet initiated from LAN, the Gigabit Router will firstly compare the packet with the bindings in the **IP/MAC Binding List**, and then process the packet according to the related configuration. The packet will be allowed to pass or be dropped immediately. If it is allowed to pass, the packet will be further processed by other function modules.

6.2.6 Internet Whitelist and Blacklist

6.2.6.1 Introduction to Internet Whitelist and Blacklist Based on IP/MAC Binding

By utilizing IP/MAC binding feature, you can flexibly configure an Internet whitelist or blacklist for the LAN users.

If you want to allow only a small number of LAN users to access the Internet, you can configure an Internet whitelist for these users. Then all users cannot access the Internet, except those listed in the whitelist.

If you want to block only a small number of LAN users from accessing the Internet, you can configure an Internet blacklist for these users. Then all users can access the Internet, except those listed in the blacklist.

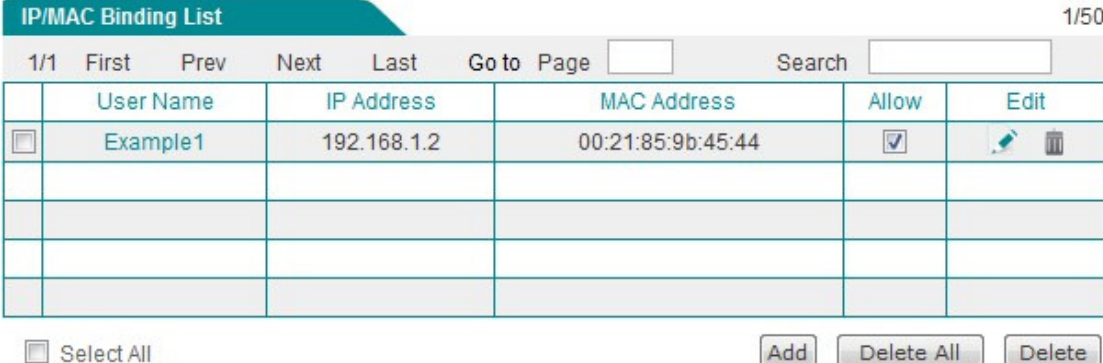
On the Gigabit Router, a user listed in the whitelist is a legal user, i.e., the user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is checked. A user listed in the blacklist is an illegal user, i.e., the user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is cleared; or the IP address or MAC address is the same as that of an IP/MAC binding, but not both.

6.2.6.2 How to Configure an Internet Whitelist

To configure an Internet whitelist, follow these steps:

- Step 1** Go to the **Advanced > IP/MAC Binding** page, and click the **Add** button to go to the **IP/MAC Binding Settings** page.
- Step 2** Specify the legal users by creating the IP/MAC bindings: Add these users' IP and MAC address pairs into the **IP/MAC Binding List**. By default, an IP/MAC binding's **Allow** check box is checked, which means that the user matching the IP/MAC binding can access the Gigabit Router and Internet, so please leave the default value. Refer to **Section 7.2.4 IP/MAC Binding Settings** for detailed information.
- Step 3** Clear the **Allow Undefined LAN PCs** check box to block all the undefined users from accessing the Gigabit Router and Internet.

For example, if you want to allow a local computer with IP address 192.168.1.2 and MAC address 0021859b4544 to access the Gigabit Router and Internet, you can add its IP/MAC address pair into the **IP/MAC Binding List**, see Figure 6-15. The binding's **Allow** check box is checked by default, so please leave the default value.



1/1	First	Prev	Next	Last	Go to Page		Search	
☐	User Name	IP Address	MAC Address	Allow	Edit			
☐	Example1	192.168.1.2	00:21:85:9b:45:44	☒	 			

☐ Select All Add Delete All Delete

Figure 6-15 IP/MAC Binding List - Example 1

6.2.6.3 How to Configure an Internet Blacklist

To configure an Internet blacklist, follow these steps:

- Step 1** Go to the **Advanced > IP/MAC Binding** page, and click the **Add** button to go to the **IP/MAC Binding Settings** page.
- Step 2** Specify the illegal users by creating the IP/MAC bindings. There are two methods (Refer to **Section 7.2.4 IP/MAC Binding Settings** for detailed information.):

- 1) **Method One:** Bind each illegal user's IP address to a MAC address which is different from any local computer's, and add these IP/MAC address pairs into the **IP/MAC Binding List**.
- 2) **Method Two:** Add these users' IP and MAC address pairs into the **IP/MAC Binding List**, and clear each IP/MAC binding's **Allow** check box respectively. Thus the matched users cannot access the Gigabit Router and Internet.

Step 3 Select the **Allow Undefined LAN PCs** check box to allow all the undefined users to access the Gigabit Router and Internet.

For example, if you want to block a local computer with IP address 192.168.1.3 from accessing the Gigabit Router and Internet, you can add an IP/MAC binding into the **IP/MAC Binding List**: the **IP Address** is 192.168.1.3, and the **MAC Address** is different from any local computer's MAC address (112233445566 here), see Figure 6-16.

IP/MAC Binding List						1/50
1/1	First	Prev	Next	Last	Go to Page	Search
	User Name	IP Address	MAC Address	Allow	Edit	
☐	Example2	192.168.1.3	11:22:33:44:55:66	☒	 	

☐ Select All Add Delete All Delete

Figure 6-16 IP/MAC Binding List - Example 2

Another example is that if you want to block a local computer with IP address 192.168.1.3 and MAC address 0021859b2564 from accessing the Gigabit Router and Internet, you can add its IP/MAC address pair into the **IP/MAC Binding List**, next clear the binding's **Allow** check box, see Figure 6-17.

IP/MAC Binding List						1/50
1/1	First	Prev	Next	Last	Go to Page	Search
	User Name	IP Address	MAC Address	Allow	Edit	
☐	Example3	192.168.1.3	00:21:85:9b:25:64	☐	 	

☐ Select All Add Delete All Delete

Figure 6-17 IP/MAC Binding List - Example 3

6.3 Static Route

This section describes the **Advanced > Static Route** page, where you can configure and view static routes.

6.3.1 Introduction to Static Route

A static route is manually configured by the network administrator, which is stored in a routing table. By using routing table, the Gigabit Router can select an optimal transmission path for each received packet, and forward the packet to the destination site effectively. The proper usage of static routes can not only improve the network performance, but also achieve other benefits, such as traffic control, provide a secure network environment.

The disadvantage of using static routes is that they cannot dynamically adapt to the current operational state of the network. When there is a change in the network or a failure occurs, some static routes will be unreachable. In this case, the network administrator should update the static routes manually.

6.3.2 Static Route List

Static Route List								1/253
1/1	First	Prev	Next	Last	Go to Page		Search	
	Name	Status	Destination IP	Subnet Mask	Gateway IP Address	Priority	Interface	Edit
☐	Route-1	Enabled	200.200.202.0	255.255.255.0	200.200.202.254	0	WAN2	 
☐								
☐								
☐								
☐								

☐ Select All Add Delete All Delete

Figure 6-18 Static Route List

- **Add a Static Route:** To add a new static route, first click the **Add** button to go to the setup page, next configure it, lastly click the **Save** button.
- **View Static Route(s):** When you have configured one or more static routes, you can view them in the **Static Route List**.
- **Modify a Static Route:** To modify a configured static route, click its **Name** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it,

and click the **Save** button.

► **Delete Static Route(s):** There are three ways to delete static route(s).

1. To delete a static route, directly click its  icon.
2. To delete more than one static route at a time, select the leftmost check boxes of the static routes that you want to delete, and then click the **Delete** button.
3. To delete all the static routes at a time, directly click the **Delete All** button.

6.3.3 Static Route Settings



The form displays the configuration for a static route named 'Route-1'. It includes fields for 'Destination IP' (200.200.202.0), 'Subnet Mask' (255.255.255.0), 'Gateway IP Address' (200.200.202.254), and 'Priority' (0). The 'Enable' checkbox is checked. The 'Interface' is set to 'WAN2'. A note below the priority field states: 'The smaller the number, the higher the priority.' At the bottom are 'Save', 'Cancel', and 'Back' buttons.

Name *	Route-1
Enable	☒
Select the check box to make the static route take effect.	
Destination IP *	200.200.202.0
Subnet Mask *	255.255.255.0
Gateway IP Address *	200.200.202.254
Priority *	0
The smaller the number, the higher the priority.	
Interface	WAN2 ▼
Save Cancel Back	

Figure 6-19 Static Route Settings

- ◆ **Name:** It specifies a unique name of the static route.
- ◆ **Enable:** It allows you to enable or disable the static route. The default value is checked, which means the static route is in effect. If you want to disable the static route temporarily instead of deleting it, please clear the check box.
- ◆ **Destination IP:** It specifies the IP address of the destination network or destination host.
- ◆ **Subnet Mask:** It specifies the subnet mask associated with the destination network.
- ◆ **Gateway IP Address:** It specifies the IP address of the next hop gateway or router to which to forward the packets.
- ◆ **Priority:** It specifies the priority of the static route. If there are multiple routes to the same destination with different priorities, the Gigabit Router will choose the route with the highest priority to forward the packets. The smaller the number, the higher the priority.

- ◆ **Interface:** It specifies an outbound interface through which the packets are forwarded to the next hop gateway or router. The available options are LAN, WAN1, APClient and 3G.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Static Route List**.

6.3.4 How to Add Static Routes

To add one or more static routes, follow these steps:

- Step 1** Go to the **Advanced > Static Route** page, and click the **Add** button to go to the setup page.
- Step 2** Specify the **Name** for the static route, and leave the **Enable** check box checked.
- Step 3** Specify the **Destination IP**, **Subnet Mask**, and **Gateway IP Address**.
- Step 4** Specify the **Priority** as required.
- Step 5** Select an outbound interface from the **Interface** drop-down list as required.

For example, if you want to add a static route for the network 192.168.1.0/24 pointing to 192.168.1.254, please choose **LAN** as the outbound interface. The following figure shows the detailed settings.

Name * Example1

Enable ☒

Select the check box to make the static route take effect

Destination IP * 192.168.1.0

Subnet Mask * 255.255.255.0

Gateway IP Address * 192.168.1.254

Priority * 0

The smaller the number, the higher the priority.

Interface LAN

Save Cancel Back

Figure 6-20 Static Route Settings - Example

- Step 6** Click the **Save** button to save the settings. You can view the static route in the

Static Route List.

Step 7 To add another new static route, please repeat the above steps.

**Note**

If you want to delete static route(s), please follow the ways described in **Section 7.3.2 Static Route List**.

6.4 PPPoE Server

This section describes how to configure PPPoE server global settings and PPPoE account settings, and how to view PPPoE user status.

6.4.1 PPPoE Overview

The PPPoE stands for Point-to-Point Protocol over Ethernet, which uses client/server model. The PPPoE provides the ability to connect the Ethernet hosts to a remote Access Concentrator (AC) over a simple bridging access device. And it provides extensive access control management and accounting benefits to ISPs and network administrators.

The PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames to provide point-to-point connection over an Ethernet network.

6.4.1.1 PPPoE Stages

As specified in RFC 2516, the PPPoE has two distinct stages: a discovery stage and a PPP session stage. The following describes them respectively.

6.4.1.2 PPPoE Discovery Stage

In the PPPoE discovery stage, a PPPoE client will find a proper server, and then build the connection. When a client initiates a PPPoE session, it should perform discovery to identify the PPPoE server's Ethernet MAC address, and establish a PPPoE session ID.

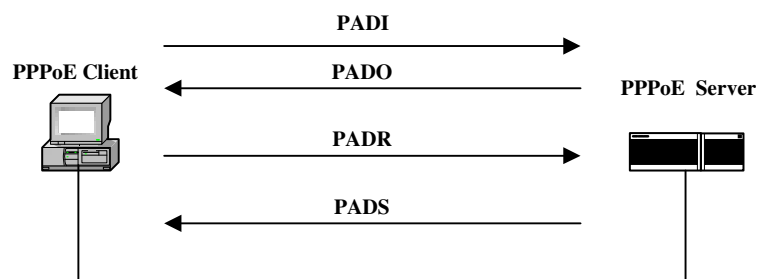


Figure 6-21 PPPoE Discovery Stage Flows

As shown in Figure 7-21, the discovery stage includes the following four steps:

1. **PADI (PPPoE Active Discovery Initiation):** At the beginning, a PPPoE client

broadcasts a PADI packet to find all the servers that can be connected possibly. Until it receives PADO packets from one or more servers. The PADI packet must contain a service name which indicates the service requested by the client.

2. **PADO (PPPoE Active Discovery Offer):** When a PPPoE server receives a PADI packet in its service range, it will send a PADO response packet. The PADO packet must contain the server's name, and a service name identical to the one in the PADI, and any number of other service names which indicate other services that the PPPoE server can offer. If a PPPoE server receives a PADI packet beyond its service range, it cannot respond with a PADO packet.
3. **PADR (PPPoE Active Discovery Request):** The client may receive more than one PADO packet as the PADI was broadcast. The client chooses one server according to the server's name or the services offered. Then the client sends a PADR packet to the selected server. The PADR packet must contain a service name which indicates the service requested by the client.
4. **PADS (PPPoE Active Discovery Session- confirmation):** When a PPPoE server receives a PADR packet; it prepares to begin a PPP session. It generates a unique PPPoE session ID, and respond to the client with a PADS packet. The PADS packet must contain a service name which indicates the service provided to the client.

When the discovery stage completes successfully, both the server and client know the PPPoE session ID and the peer's Ethernet MAC address, which together define the PPPoE session uniquely.

6.4.1.3 PPP Session Stage

In the PPP session stage, the server and client perform standard PPP negotiation to establish a PPP connection. After the PPP connection is established successfully, the original datagram are encapsulated in PPP frames, and PPP frames are encapsulated in PPPoE session frames, which have the Ethernet type 0x8864. Then these Ethernet frames are sent to the peer. In a PPPoE session frame, the session ID must be the value assigned in the Discovery stage, and cannot be changed in this session.

6.4.1.4 PPPoE Session Termination

After a session is established, either the server or client may send a PADT (PPPoE Active Discovery Terminate) packet at anytime to indicate the session has been terminated. The PADT packet's SESSION-ID must be set, to indicate which session is to be terminated. Once received a PADT, no further PPP packets (even normal PPP termination packets) are allowed to be sent using the specified session. A PPP peer should use the PPP protocol itself to terminate a PPPoE session, but can use the PADT packet to terminate the PPPoE session if PPP cannot be used.

6.4.2 PPPoE Server Global Settings

Enable PPPOE Server ☒

To make the PPPoE server related settings take effect, select the check box to enable PPPoE server.

Start IP Address * 10.10.10.1

Primary DNS Server * 202.96.199.133

Secondary DNS Server

You can find DNS server addresses in Start > System Status.

PPP Authentication AUTO ▼

Maximum Sessions * 50

Save Cancel

Figure 6-22 PPPoE Server Global Settings

- ◆ **Enable PPPoE Server:** It allows you to enable or disable PPPoE server. If you want to enable PPPoE server on the Gigabit Router, please select this check box.
- ◆ **Start IP Address:** It specifies the starting IP address that is assigned by the PPPoE server.
- ◆ **Primary DNS Server:** It specifies the IP address of the primary DNS server that is available to a PPPoE client.
- ◆ **Secondary DNS Server:** It specifies the IP address of the secondary DNS server that is available to a PPPoE client.
- ◆ **PPP Authentication:** It specifies the PPP authentication mode by which the PPPoE server authenticates a PPPoE client. The available options are **PAP**, **CHAP** and **AUTO**. In most cases, please leave the default value of **AUTO**, which means that the Gigabit Router will automatically choose **PAP** or **CHAP** to authenticate the PPPoE client.
- ◆ **Maximum Sessions:** It specifies the maximum number of PPPoE sessions that can be created on the Gigabit Router.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

6.4.3 PPPoE Account List

PPPoE Account List1/50

1/1FirstPrevNextLastGo to PageSearch

	User Name	Static IP Address	Edit
☐	test	10.10.10.10	 

☐ Select All

AddDelete AllDelete

Figure 6-23 PPPoE Account List

- ▶ **Add a PPPoE Account:** To add a new PPPoE account, first click the **Add** button to go to the setup page, next configure it, lastly click the **Save** button.
- ▶ **View PPPoE Account(s):** When you have configured one or more PPPoE accounts, you can view them in the **PPPoE Account List**.
- ▶ **Modify a PPPoE Account:** To modify a configured PPPoE account, click its **User Name** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete PPPoE Account(s):** There are three ways to delete PPPoE account(s).
 1. To delete a PPPoE account, directly click its  icon.
 2. To delete more than one PPPoE account at a time, select the leftmost check boxes of the PPPoE accounts that you want to delete, and then click the **Delete** button.
 3. To delete all the PPPoE accounts at a time, directly click the **Delete All** button.

6.4.4 PPPoE Account Settings

Go to the **Advanced > PPPoE Server > PPPoE Account Settings** page, and click the **Add** button to go to the setup page shown in Figure 6-24.



User Name * test

Password * ●●●●●●

Confirm Password * ●●●●●●

Static IP Address 10.10.10.10

Save Cancel Back

Figure 6-24 PPPoE Account Settings

- ◆ **User Name:** It specifies a unique user name of the PPPoE account. It must be between 1 and 31 characters long. The PPPoE server will use **User Name** and **Password** to identify the PPPoE client.
- ◆ **Password:** It specifies the password of the PPPoE account.
- ◆ **Confirm Password:** You should re-enter the password.
- ◆ **Static IP Address:** It specifies a static IP address that is assigned to the user who uses the current PPPoE account. It must be a valid IP address within the range of IP addresses assigned by the PPPoE server.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **PPPoE Account List**.

6.4.5 PPPoE User Status

You can go to the **Advanced > PPPoE Server > PPPoE User Status** page view the status information of online PPPoE dial-in users in the **PPPoE User Status List**, which include the user name, assigned IP address, MAC address, Rx rate and Tx rate, and online time.

PPPoE User Status List						1/50
1/1	First	Prev	Next	Last	Go to Page	Search
User Name	IP Address	MAC Address	Online Time	Tx Rate (KB/s)	Rx Rate (KB/s)	
mary	1.1.1.2	1C:6F:65:ED:8A:12	0:1:0	1	2	

Figure 6-25 PPPoE User Status List

- ◆ **User Name:** It displays the user name of the PPPoE account. The PPPoE dial-in user uses it to dial-up and establish the PPPoE session to the Gigabit Router.
- ◆ **IP Address:** It displays the PPPoE dial-in user's IP address assigned by the PPPoE server.
- ◆ **MAC Address:** It displays the PPPoE dial-in user's MAC address.
- ◆ **Online Time:** It displays the elapsed time since the PPPoE session was established.
- ◆ **Tx Rate:** It displays the real-time upload rate (in kilobytes per second) of the PPPoE dial-in user.
- ◆ **Rx Rate:** It displays the real-time download rate (in kilobytes per second) of the PPPoE dial-in user.
- ▶ **Refresh:** Click to view the latest information in the list.

Chapter 7 User Management

This chapter describes how to control and manage the Internet behaviors of the LAN users, including global management and group management.

7.1 Global Management

This section describes the **User > Global Management** page.

In this page, you can easily control and manage the Internet behaviors of the LAN users based on schedule, which include: allow or block the LAN users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., Bit Comet, Bit Spirit, Thunder Search) during the specified schedule. Using P2P applications in the LAN will impact the other users accessing the Internet, even cause network congestion and performance deterioration. You can block P2P applications to avoid such situations.

7.1.1 Global Management Policy Settings

Global Policy Settings

Block QQ ☐ [\[Update Policy\]](#)

Block MSN ☐ [\[Update Policy\]](#)

Block BT ☐ [\[Update Policy\]](#)

Block Thunder Search ☐ [\[Update Policy\]](#)

Schedule

Days ☒ Everyday
☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time ☒ 24 Hours
☐ From : To :

Figure 7-1 Global Management Policy Settings

- ◆ **Block QQ:** It allows or blocks QQ application. If you want to block the LAN users from using QQ to chat with others, please select this check box.
- ◆ **Block MSN:** It allows or blocks MSN Messenger. If you want to block the LAN users from using MSN Messenger to chat with others, please select this check box.
- ◆ **Block BT:** It allows or blocks BitSpirit and BitComet applications. If you want to block the LAN users from using BitSpirit or BitComet to download files, please select this check box.
- ◆ **Block Thunder Search:** It allows or blocks Thunder search application. If you want to block the LAN users from using Thunder to search resources, please select this check box.
- ◆ **Schedule:** It allows you to define a schedule to restrict when the global management policy is in effect. By default, it is always in effect.
 - **Days:** It specifies the day(s) of the week during which the schedule is in effect. By default, the **Everyday** check box is checked, which means all days of the week. You may clear the **Everyday** check box, and then select any single day (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday) or combinations of days as desired.
 - **Time:** It specifies a range of hours and minutes during which the schedule is in effect. By default, the **24 Hours** check box is checked, which means the schedule is in effect all day on the selected day(s). You may clear the **24 Hours** check box, and then choose the daily start time and end time as desired. If the start time is later than the end time, the system will automatically divide it into two time periods. E.g., if you select the **Mon** check box, and choose **23:00** and **06:00** as the daily start time and end time respectively, the schedule will be in effect during 00:00~06:00 and 23:00~23:59 on Monday.
- ▶ **Update Policy:** Click to update the corresponding policy. If you click the **Update Policy** hyperlink, the system will jump to the **Update Policy** page (see Figure 7-2), and go back to the **User > Global Management** page after the update is complete.

Updating policy, please wait ...

Remaining 8 seconds.

Figure 7-2 Updating Policy

- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.



Note

The global management policy applies to the LAN users whose IP address is on the same subnet as the Gigabit Router's LAN interface, and PPPoE dial-in users. Other users aren't subject to the policy.

7.1.2 An Example for Global Management Policy

A business uses a HiPER 840G Gigabit Router to access the Internet. The CEO wants to block the employees from using MSN and BT applications during business hours (Monday to Friday, 9:00 to 17:00).

The configuration steps are the following:

- Step 1** Go to the **User > Global Management** page.
- Step 2** Select the **Block MSN** and **Block BT** check boxes.
- Step 3** Define business hours: clear the **Everyday** check box, next select the **Mon**, **Tue**, **Wed**, **Thu**, and **Fri** check boxes; clear the **24 Hours** check box, next choose **09:00** and **17:00** as the daily start time and end time respectively. The above settings are shown in Figure 7-3.
- Step 4** Click the **Save** button to save your settings.

Global Policy Settings

Block QQ	☐	[Update Policy]
Block MSN	☒	[Update Policy]
Block BT	☒	[Update Policy]
Block Thunder Search	☐	[Update Policy]

Schedule

Days ☐ Everyday

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Sun

Time ☐ 24 Hours

☒ From 09 : 00 To 17 : 00

Figure 7-3 Global Management Policy - Example

7.2 Group Management

This section describes the **User > Group Management** page.

In this page, you can group the users that have the same Internet access privileges into a user group, and assign a range of contiguous IP addresses to them. After that, you can create group management policies for each group based on schedule. For convenience, a group can also contain a single user.

A group management policy is used to control the Internet behaviors of the users in the group, which include: allow or block these users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., Bit Comet, Bit Spirit, Thunder Search) during the specified schedule; in addition, it is also used to control the maximum upload and download rate of these users during the specified schedule.

7.2.1 Group Management Policy List

Group Management List								3/5
1/1	First	Prev	Next	Last	Go to Page		Search	
	Group Name	Start IP Address	End IP Address	Rate Limit Mode	Max. Rx Rate	Max. Tx Rate	Block	
☐	Policy-1	192.168.1.6	192.168.1.6	Each	0 bit/s	0 bit/s	No	
☐	Policy-2	192.168.1.2	192.168.1.10	Each	0 bit/s	0 bit/s	Yes	
☐	Policy-3	192.168.1.11	192.168.1.30	Each	0 bit/s	0 bit/s	No	

☐ Select All

Figure 7-4 Group Management Policy List

Group Management List								3/5
1/1	First	Prev	Next	Last	Go to Page		Search	
Max. Rx Rate	Max. Tx Rate	Block QQ	Block MSN	Block BT	Block Thunder Search	Schedule	Edit	
0 bit/s	0 bit/s	No	No	No	No	Everyday		
0 bit/s	0 bit/s	Yes	Yes	No	No	Everyday		
0 bit/s	0 bit/s	No	No	No	No	Everyday		

☐ Select All

Figure 7-5 Group Management Policy List (Continue)

- ▶ **Add a Group Management Policy:** To add a new group management policy, first click the **Add** button to go to the **Group Management Settings** page, next configure it, lastly click the **Save** button.
- ▶ **View Group Management Policy(s):** When you have configured one or more group management policies, you can view them in the **Group Management List**.
- ▶ **Modify a Group Management Policy:** To modify a configured group management policy, click its **Group Name** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete Group Management Policy(s):** There are three ways to delete group management policy(s).
 1. To delete a group management policy, directly click its  icon.
 2. To delete more than one group management policy at a time, select the leftmost check boxes of the policies that you want to delete, and then click the **Delete** button.
 3. To delete all the group management policies at a time, directly click the **Delete All** button.

7.2.2 Group Management Policy Settings

Group Name*	Policy-2		
Start IP Address*	192.168.1.2		
End IP Address*	192.168.1.10		
Rate Limit Mode	Each (Limit each PC's rate to Max. value)		
Max. Tx Rate	0 kbit/s	<==	No Limit (0 means no limit.)
Max. Rx Rate	0 kbit/s	<==	No Limit (0 means no limit.)
Block QQ	☒	[Update Policy]	
Block MSN	☒	[Update Policy]	
Block BT	☐	[Update Policy]	
Block Thunder Search	☐	[Update Policy]	
Schedule			
Days	☒ Everyday		
	☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun		
Time	☒ 24 Hours		
	☐ From 00 : 00 To 00 : 00		
Save Cancel Back			

Figure 7-6 Group Management Policy Settings

- ◆ **Group Name:** It specifies a unique name of group.
- ◆ **Start IP Address** and **End IP Address:** They specify a range of contiguous IP addresses. All the computers within the specified range are members of the group, and are subject to the group management policy.
- ◆ **Rate Limit Mode:** It specifies the mode by which the Gigabit Router will limit the maximum Tx/Rx rate of the LAN computers belonging to the group.
 - **Each:** If you select this option, the Tx/Rx rate of each computer can reach up to the **Max. Tx Rate/ Max. Rx Rate** you specify.
 - **Share:** If you select this option, the total Tx/Rx rate of all computers in the group can reach up to the **Max. Tx Rate/ Max. Rx Rate** you specify.
- ◆ **Max. Tx Rate:** It specifies the maximum upload rate (in Kbit/s) of the LAN computers belonging to the group.
- ◆ **Max. Rx Rate:** It specifies the maximum download rate (in Kbit/s) of the LAN computers belonging to the group. There are two ways to set the **Max. Tx Rate** and **Max. Rx Rate**.
 - Enter a value in the associated text box. If you don't want to limit **Max. Tx Rate/ Max. Rx Rate**, please leave the default value of **0**.
 - Select an option from the associated drop-down list. If you don't want to **Max. Tx Rate/ Max. Rx Rate**, please leave the default value of **No Limit**.
- ◆ **Block QQ, Block MSN, Block BT, Block Thunder Search, and Schedule:** Refer to **Section 8.1.1 Global Management Policy Settings** for detailed information.
- ▶ **Update Policy:** Click to update the corresponding policy. Refer to **Section 8.1.1 Global Management Policy Settings** for detailed operation.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Group Management List**.

**Note**

1. The policy management policies take priority over the global management policy.
2. The Gigabit Router supports up to five group management policies.
3. If both **Start IP Address** and **End IP Address** are set to 0.0.0.0, the group will contain all computers on the LAN no matter what IP address they might have. In this case, the Gigabit Router will check all the packets initiated from the LAN computers, so the system performance will be degraded to some extent. Therefore, you'd better not set them to 0.0.0.0.

7.2.3 Execution Order of Group Management Policies

If a user's computer belongs to more than one group, in other words, if the user matches more than one group management policy, it will be subject to the first one added. More specifically, after you configure some group management policies, the Gigabit Router will search the **Group Management List** to find out if there is a policy matching a user. It will check the user's IP address against each policy in the order in which the policies are listed. The first matching policy will apply to the user. Note that the policies are listed in chronological order of creation (i.e., most recent at the bottom).

7.2.4 Priorities of Global and Group Management Policies and Access Rules

The access rules have higher priority than the group management policies, and the group management policies have higher priority than the global management policy. That is, when receiving a packet initiated from a local computer, the Gigabit Router will first check it against the access rules, next the group management policies, lastly the global management policy. The first rule (or policy) that matches the packet is applied. After a match is found, no further rules or policies are checked.

For example, if you have selected the **Block MSN** check box in the **User > Global Management** page, added a group management policy which allows a group of users to use MSN (**Block MSN** check box is cleared) in the **User > Group Management** page, and added an access rule which denies all users access to the Internet in the **Firewall > Access Control** page, then any users are unable to access the Internet because the access rule is matched first. Now if you only delete the access rule, then the users belong to the specified group can use MSN, but other users cannot.

7.2.5 An Example for Group Management Policy

1. Requirements

A business uses a HiPER 840G Gigabit Router to access the Internet. The CEO wants to control Internet behaviors of the employees of the Administration Department and Business Department:

- 1) Block the Administration Department's employees (IP range: 192.168.1.2-192.168.1.10) from using MSN and QQ, and allow them to access all other services.

The exception is that the CEO with IP address 192.168.1.6 can access any services.

- 2) Allow the Business Department's employees (IP range: 192.168.1.11-192.168.1.30) to access any services.

2. Analysis

We need to create three group management policies to meet the requirements:

- Group management policy 1: It allows the CEO to access all Internet services.
- Group management policy 2: It blocks the Administration Department's employees from using QQ and MSN.
- Group management policy 3: It allows the Business Department's employees to access all Internet services.

3. Configuration Steps

Step 1 Go to the **User > Group Management** page.

Step 2 Click the **Add** button to go to the **Group Management Settings** page to create the policy 1. The detailed settings are shown in Figure 7-7.

Group Name* Policy-1

Start IP Address* 192.168.1.6

End IP Address* 192.168.1.6

Rate Limit Mode Each (Limit each PC's rate to Max. value) ▼

Max. Tx Rate 0 kbit/s <== No Limit ▼ (0 means no limit.)

Max. Rx Rate 0 kbit/s <== No Limit ▼ (0 means no limit.)

Block QQ ☐ [\[Update Policy\]](#)

Block MSN ☐ [\[Update Policy\]](#)

Block BT ☐ [\[Update Policy\]](#)

Block Thunder Search ☐ [\[Update Policy\]](#)

Schedule

Days ☒ Everyday

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time ☒ 24 Hours

☐ From 00 : 00 To 00 : 00

[Save](#) [Cancel](#) [Back](#)

Figure 7-7 Group Management Policy Example - Policy 1

Step 3 Click the **Add** button to go to the **Group Management Settings** page to create the policy 2. The detailed settings are shown in Figure 7-8.

Group Name* Policy-2

Start IP Address* 192.168.1.2

End IP Address* 192.168.1.10

Rate Limit Mode Each (Limit each PC's rate to Max. value) ▼

Max. Tx Rate 0 kbit/s <== No Limit ▼ (0 means no limit.)

Max. Rx Rate 0 kbit/s <== No Limit ▼ (0 means no limit.)

Block QQ ☒ [Update Policy]

Block MSN ☒ [Update Policy]

Block BT ☐ [Update Policy]

Block Thunder Search ☐ [Update Policy]

Schedule

Days ☒ Everyday

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time ☒ 24 Hours

☐ From 00 : 00 To 00 : 00

Save Cancel Back

Figure 7-8 Group Management Policy Example - Policy 2

Step 4 Click the **Add** button to go to the **Group Management Settings** page to create the policy 3. The detailed settings are shown in Figure 7-9.

Group Name*

Start IP Address*

End IP Address*

Rate Limit Mode

Max. Tx Rate kbit/s <== (0 means no limit.)

Max. Rx Rate kbit/s <== (0 means no limit.)

Block QQ ☐ [\[Update Policy\]](#)

Block MSN ☐ [\[Update Policy\]](#)

Block BT ☐ [\[Update Policy\]](#)

Block Thunder Search ☐ [\[Update Policy\]](#)

Schedule

Days ☒ Everyday
☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time ☒ 24 Hours
☐ From : To :

Figure 7-9 Group Management Policy Example - Policy 3

Step 5 After you have configured the three policies, you can view them in the **Group Management List**, see Figure 7-10.

Group Management List							3/5
1/1	First	Prev	Next	Last	Go to Page		Search
☐	Group Name	Start IP Address	End IP Address	Rate Limit Mode	Max. Rx Rate	Max. Tx Rate	Block
☐	Policy-1	192.168.1.6	192.168.1.6	Each	0 bit/s	0 bit/s	No
☐	Policy-2	192.168.1.2	192.168.1.10	Each	0 bit/s	0 bit/s	Yes
☐	Policy-3	192.168.1.11	192.168.1.30	Each	0 bit/s	0 bit/s	No
☐							
☐							

☐ Select All

Figure 7-10 Group Management List – Example

Group Management List 3/5

1/1 First Prev Next Last Go to Page Search

Max. Rx Rate	Max. Tx Rate	Block QQ	Block MSN	Block BT	Block Thunder Search	Schedule	Edit
0 bit/s	0 bit/s	No	No	No	No	Everyday	 
0 bit/s	0 bit/s	Yes	Yes	No	No	Everyday	 
0 bit/s	0 bit/s	No	No	No	No	Everyday	 

☐ Select All

Figure 7-11 Group Management List – Example (Continue)

Chapter 8 Firewall

This chapter describes how to configure firewall features, including access control, domain filtering, and attack prevention.

8.1 Access Control

This section describes the **Firewall > Access Control** page, which includes the **Access Rule List** and **Access Rule Settings**.

8.1.1 Introduction to Access Control

8.1.1.1 The Purpose of Access Control Feature

By flexibly utilizing access control, you can not only assign different Internet access privileges to different LAN users, but also assign different Internet access privileges to the same users based on schedules. In practice, you can set appropriate access rules according to the actual requirements of your organization. Such as, for a school, you can block the students from accessing game websites; for a family, you can only allow your children to access the Internet during the specified period of time; for a business, you can block the Financial Department's employees from accessing the Internet.

8.1.1.2 The Operation Principle of Access Control

By default, the Gigabit Router will forward all the valid packets received by the LAN interface because no access rule exists. After you have configured some access rules, the Gigabit Router will examine each packet received by the LAN interface to determine whether to forward or drop it, based on the criteria you specified in the access rules.

More specifically, when receiving a packet initiated from LAN, the Gigabit Router will analyze the packet by extracting its source MAC address, source IP address, destination IP address, protocol type, port number, content, and the date and time at which the packet was received, and then compare them with each rule in decreasing order of priority. The

first rule that matches the packet is applied, and the specified **Action** (**Allow** or **Deny**) is taken. After a match is found, no further rules are checked. Note that the rules are listed in decreasing order of priority in the **Access Rule List**: The rule with a higher priority is listed before the one with a lower priority.

8.1.1.3 Filtering Type of Access Rule

The Gigabit Router supports three filtering types of access rule, which include IP filtering, URL filtering and keyword filtering. All of them support access control based on schedule.

1. IP Filtering

The IP filtering rules are used to filter IP packets based on the packet header information, such as source IP address, destination IP address, protocol type (TCP, UDP, ICMP, etc.), TCP/UDP source port and destination port.

The filtering criteria that you can specify within an IP filtering rule include: source IP address, destination IP address, protocol, source port, destination port, and schedule.

2. URL Filtering

The URL filtering rules are used to filter URLs based on keyword in the URL. It allows you to filter any web page whose URL contains the specified keyword. For example, if you want to block sex related websites, you can use the URL keyword “sex”. This will block any web page whose URL contains sex, such as www.sexpicture.com. Of course, you can use the full URL (like “www.yahoo.com”) to filter only the specified URL.

The filtering criteria that you can specify within a URL filtering rule include: source IP address, filtering content (i.e., URL keyword), and schedule.

3. Keyword Filtering

The keyword filtering rules are used to block users from submitting information to the web page based on keyword, that is, the information that contains the specified keyword (such as pornography, gambling, etc.) cannot be submitted to any web page. The Gigabit Router supports both Chinese and English keyword filtering.

The filtering criteria that you can specify within a keyword filtering rule include: source IP address, filtering content (i.e., keyword in the web page), and schedule.

8.1.1.4 Action of Access Rule

The action of an access rule is either **Allow** or **Deny**. As mentioned earlier, the Gigabit

Router checks each received packet against the access rules in the **Access Rule List**, and the first access rule that matches a packet determines whether the Gigabit Router accepts or drops the packet. If the rule's **Action** is **Allow**, the packet is forwarded. If the rule's **Action** is **Deny**, the packet is dropped.

Note that keyword filtering rules only support the **Deny** action.

8.1.2 Access Rule List

Access Rule List								3/100
1/1	First	Prev	Next	Last	Go to Page		Search	
	Name	Status	Source IP Range	Priority	Action	Schedule	Filtering Type	
☐	Rule-1	Enabled	192.168.1.10–192.168.1.20	5	Deny	Everyday	URL Filtering	ht
☐	Rule-2	Enabled	192.168.1.10–192.168.1.20	11	Allow	Everyday	IP Filtering	
☐	Rule-3	Enabled	192.168.1.10–192.168.1.20	12	Deny	Everyday	Keyword Filtering	

☐ Select All

Figure 8-1 Access Rule List

Access Rule List							3/100
1/1	First	Prev	Next	Last	Go to Page		Search
Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port End	Dest IP Start	Dest IP End	
URL Filtering	www.bbc.com						
IP Filtering		TCP	80	80	0.0.0.0	0.0.0.0	
Keyword Filtering	gambling						

☐ Select All

Figure 8-2 Access Rule List (Continue)

Access Rule List							3/100
1/1	First	Prev	Next	Last	Go to Page		Search
Port Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit	
80	80	0.0.0.0	0.0.0.0	1	65535		
							

☐ Select All

Figure 8-3 Access Rule List (Continue)

- ▶ **Add an Access Rule:** To add a new access rule, first click the **Add** button to go to the **Access Rule Settings** page, next configure it, lastly click the **Save** button.
- ▶ **View Access Rule(s):** When you have configured one or more access rules, you can view them in the **Access Rule List**.
- ▶ **Modify an Access Rule:** To modify a configured access rule, click its **Name** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete Access Rule(s):** There are three ways to delete access rule(s).
 1. To delete a access rule, directly click its  icon.
 2. To delete more than one access rule at a time, select the leftmost check boxes of the access rules that you want to delete, and then click the **Delete** button.
 3. To delete all the access rules at a time, directly click the **Delete All** button.

8.1.3 Access Rule Settings

The following sections describe three types of access rule respectively, which include IP filtering, URL filtering and keyword filtering.

8.1.3.1 Access Rule Settings - IP Filtering

Name*

Enable ☒

Select the check box to make the access rule take effect.

Source IP Range* To *

A group of LAN PCs to which the rule applies.

Priority*

The smaller the number, the higher the priority.

Action

Filtering Type

Protocol

Predefined Service

Dest Port Start* Dest Port End*

Dest IP Start Dest IP End

Source Port Start Source Port End

Schedule

Days ☒ Everyday

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time ☒ 24 Hours

☐ From : To :

Figure 8-4 Access Rule Settings - IP Filtering

- ◆ **Name:** It specifies a unique name of the access rule.
- ◆ **Enable:** It allows you to enable or disable the access rule. The default value is checked, which means the access rule is in effect. If you want to disable the rule temporarily instead of deleting it, please clear the check box.
- ◆ **Source IP Range:** It specifies a range of source IP addresses (i.e., a group of local computers) to which the access rule applies. To specify a single local computer, enter its address in both text boxes.
- ◆ **Priority:** It specifies the priority of the access rule. The access rules will be checked against the packets in descending order of priority. It must be between 0 and 100. The smaller the number, the higher the priority. And the priority of each access rule cannot

be repeated.

- ◆ **Action:** It specifies the action to be taken if a packet matches the access rule. The available options are **Allow** and **Deny**.
 - **Allow:** It indicates that the Gigabit Router will allow the packets matching the rule, that is, the Gigabit Router will forward these packets.
 - **Deny:** It indicates that the Gigabit Router will deny the packets matching the rule, that is, the Gigabit Router will drop these packets.
- ◆ **Filtering Type:** It specifies the filtering type of the access rule. The options are **IP Filtering**, **URL Filtering**, and **Keyword Filtering**. Here please select **IP Filtering**.
- ◆ **Protocol:** It specifies the protocol to which the access rule applies. The options are **1 (ICMP)**, **6 (TCP)**, **17 (UDP)**, **51 (AH)**, and **All**. Select **All** if you want the rule to apply to all protocols. **Appendix C** provides the list of common IP protocols and their protocol numbers.
- ◆ **Predefined Service:** It provides some of the most common services and their associated port numbers. Select **All** if you want the rule to apply to all ports (1-65535). **Appendix D** provides the list of common services and their port numbers.
- ◆ **Dest Port Start** and **Dest Port End:** They specify a range of destination ports to which the access rule applies. To specify a single port, enter the port number in both text boxes. The port number must be between 1 and 65535.
- ◆ **Dest IP Start** and **Dest IP End:** They specify a range of destination IP addresses to which the access rule applies. To specify a single IP address, enter the port number in both text boxes.
- ◆ **Source Port Start** and **Source Port End:** They specify a range of source ports to which the access rule applies. To specify a single port, enter the port number in both text boxes. The port number must be between 1 and 65535.
- ◆ **Schedule:** It allows you to specify when the access rule is in effect. By default, the access rule is always in effect.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Access Rule List**.



Note

By default, the **Source IP Range** is from 0.0.0.0 to 0.0.0.0, which means the access rule applies to all computers on the LAN no matter what IP address they might have. In this case, the Gigabit Router will check any packets initiated from the LAN computers, so the system performance will be degraded to some extent. Therefore, you'd better change the default value.

8.1.3.2 Access Rule Settings - URL Filtering

Name*

Enable ☒

Select the check box to make the access rule take effect.

Source IP Range* To *

A group of LAN PCs to which the rule applies.

Priority*

The smaller the number, the higher the priority.

Action

Filtering Type

Filtering Content*

Schedule

Days ☒ Everyday

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time ☒ 24 Hours

☐ From : To :

Figure 8-5 Access Rule Settings - URL Filtering

The parameters **Name**, **Source IP Range**, **Priority** and **Action**, and **Schedule** related parameters are the same as those of the **IP Filtering** access rule, please refer to **Section 9.1.3.1 Access Rule Settings - IP Filtering** for detailed information.

◆ **Filtering Type:** It specifies the filtering type of the access rule. The options are **IP Filtering**, **URL Filtering**, and **Keyword Filtering**. Here please select **URL Filtering**.

◆ **Filtering Content:** It specifies the URL keyword that you want to filter. The access rule is used to filter any web pages whose URL contains the specified keyword.

You can enter part of a URL to match all URLs that contain that string, or you can enter the full URL to match only the specified URL. Here we give two examples.

Example 1: If you enter **yahoo**, it will match any URL that contains yahoo, such as <http://www.yahoo.com>, <http://news.yahoo.com/>, <http://cn.yahoo.com/>, and so on.

Example 2: If you enter **news.yahoo.com**, it will match <http://news.yahoo.com/> and all URLs that start with news.yahoo.com, such as <http://news.yahoo.com/education/>. However, it won't match <http://www.yahoo.com> and <http://cn.yahoo.com/>.

- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Access Rule List**.



Note

1. The URL keyword that you enter in the **Filtering Content** text box is case insensitive, and it needn't include http://.
2. The URL filtering rules cannot be used to control users' access to other services through a web browser. For example, to control users' access to ftp://ftp.utt.com.cn, you need to configure an IP filtering rule to allow or deny ftp service.

8.1.3.3 Access Rule Settings - Keyword Filtering

Name*

Enable ☒

Select the check box to make the access rule take effect.

Source IP Range* To *

A group of LAN PCs to which the rule applies.

Priority*

The smaller the number, the higher the priority.

Action

Filtering Type

Filtering Content*

Schedule

Days ☒ Everyday

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Time ☒ 24 Hours

☐ From : To :

Figure 8-6 Access Rule Settings - Keyword Filtering

The parameters **Name**, **Source IP Range**, **Priority** and **Action**, and **Schedule** related parameters are the same as those of the **IP Filtering** access rule, please refer to **Section**

9.1.3.1 Access Rule Settings - IP Filtering for detailed information.

- ◆ **Filtering Type:** It specifies the filtering type of the access rule. The options are **IP Filtering**, **URL Filtering**, and **Keyword Filtering**. Here please select **Keyword Filtering**.
- ◆ **Filtering Content:** It specifies the keyword that you want to block. The access rule is used to block users from submitting any information that contains the specified keyword to any web page. The Gigabit Router supports both Chinese and English keyword filtering. A keyword must be a single word without white space.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Access Rule List**.



Note

1. The keyword filtering rules only support the **Deny** action.
2. The English keyword is case sensitive.

8.1.4 Configuration Examples for Access Rule

8.1.4.1 Example 1 - Only Allow a Group of Users to Access Certain Services

In this example, we want to allow a group of users (IP address range: 192.168.1.10-192.168.1.20) to access web service, and block them from accessing any other services.

We need to create three access rules to meet the requirements:

- Access rule 1: It allows those users to access DNS service. And it is used to ensure that the domain names can be resolved successfully, thus the users can access web service properly.
- Access rule 2: It allows those users to access Web service.
- Access rule 3: It blocks those users from accessing any Internet services.

Therein, both rule 1 and rule 2 must have a higher priority than rule 3. Otherwise, rule 3 will be matched first. This will make those users unable to access web service.

Access Rule List								3/100
1/1	First	Prev	Next	Last	Go to Page		Search	
	Name	Status	Source IP Range	Priority	Action	Schedule	Filtering Type	Filter
☐	Rule-1	Enabled	192.168.1.10--192.168.1.20	5	Allow	Everyday	IP Filtering	
☐	Rule-2	Enabled	192.168.1.10--192.168.1.20	10	Allow	Everyday	IP Filtering	
☐	Rule-3	Enabled	192.168.1.10--192.168.1.20	15	Deny	Everyday	IP Filtering	
☐								
☐								

☐ Select All

Figure 8-7 Access Rule List - Example 1

Access Rule List							3/100
1/1	First	Prev	Next	Last	Go to Page		Search
Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port End	Dest IP Start	Dest IP End	
IP Filtering		UDP	53	53	0.0.0.0	0.0.0.0	
IP Filtering		TCP	80	80	0.0.0.0	0.0.0.0	
IP Filtering		all	0	0	0.0.0.0	0.0.0.0	

☐ Select All

Figure 8-8 Access Rule List - Example 1 (Continue)

Access Rule List							3/100
1/1	First	Prev	Next	Last	Go to Page		Search
Dest Port Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit	
	53	0.0.0.0	0.0.0.0	1	65535	 	
	80	0.0.0.0	0.0.0.0	1	65535	 	
	0	0.0.0.0	0.0.0.0	0	0	 	

☐ Select All

Figure 8-9 Access Rule List - Example 1 (Continue)

8.1.4.2 Example 2 - Only Block a Group of Users from Accessing Certain Services

In this example, we want to block a group of users (IP address range: 192.168.1.80-192.168.1.100) from accessing www.bbc.com and www.cnn.com, and allow them to

access any other services. We need to create three access rules to meet the requirements:

- Access rule 1: It blocks those users from accessing www.bbc.com.
- Access rule 2: It blocks those users from accessing www.cnn.com.
- Access rule 3: It allows those users to access all Internet services.

Therein, both rule 1 and rule 2 must have a higher priority than rule 3. Otherwise, rule 3 will be matched first. This will make those users unable to access www.bbc.com and www.cnn.com.

Access Rule List								3/100
1/1	First	Prev	Next	Last	Go to Page		Search	
	Name	Status	Source IP Range	Priority	Action	Schedule	Filtering Type	Filtering Content
☐	Rule-1	Enabled	192.168.1.80--192.168.1.100	10	Deny	Everyday	URL Filtering	www.bbc.com
☐	Rule-2	Enabled	192.168.1.80--192.168.1.100	11	Deny	Everyday	URL Filtering	www.cnn.com
☐	Rule-3	Enabled	192.168.1.80--192.168.1.100	12	Allow	Everyday	IP Filtering	
☐								
☐								

☐ Select All

Figure 8-10 Access Rule List - Example 2

Access Rule List								3/100
1/1	First	Prev	Next	Last	Go to Page		Search	
Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port End	Dest IP Start	Dest IP		
URL Filtering	www.bbc.com							
URL Filtering	www.cnn.com							
IP Filtering		all	0	0	0.0.0.0	0.0.0		

☐ Select All

Figure 8-11 Access Rule List - Example 2 (Continue)

Access Rule List								3/100
1/1	First	Prev	Next	Last	Go to Page		Search	
Port Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit		
	0	0.0.0.0	0.0.0.0	0	0			

☐ Select All

Figure 8-12 Access Rule List - Example 2 (Continue)

8.1.4.3 Example 3 - Control Internet Behaviors of a Group of Users based on Schedule

In this example, we want to only allow a group of users (IP address range: 192.168.1.150 -192.168.1.200) to access web service during business hours (Monday to Friday, 9:00 to 17:00), and block them from accessing any Internet services during rest periods.

We need to create three access rules to meet the requirements:

- Access rule 1: It allows those users to access DNS service during business hours. And it is used to ensure that the domain names can be resolved successfully, thus the users can access web service properly.
- Access rule 2: It allows those users to access web service during business hours.
- Access rule 3: It blocks those users from accessing any Internet services.

Therein, both rule 1 and rule 2 must have a higher priority than rule 3. Otherwise, rule 3 will be matched first. This will make those users unable to access web service during business hours.

Access Rule List							3/100
1/1	First	Prev	Next	Last	Go to Page		Search
	Name	Status	Source IP Range	Priority	Action	Schedule	F
☐	Rule-1	Enabled	192.168.1.150--192.168.1.200	20	Allow	Mon,Tue,Wed,Thu,Fri;09:00-17:00	
☐	Rule-2	Enabled	192.168.1.150--192.168.1.200	21	Allow	Mon,Tue,Wed,Thu,Fri;09:00-17:00	
☐	Rule-3	Enabled	192.168.1.150--192.168.1.200	22	Deny	Everyday	

☐ Select All

Figure 8-13 Access Rule List - Example 3

Access Rule List							3/100
1/1	First	Prev	Next	Last	Go to Page		Search
Schedule	Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port End		
Mon,Tue,Wed,Thu,Fri;09:00-17:00	IP Filtering		UDP	53	53		
Mon,Tue,Wed,Thu,Fri;09:00-17:00	IP Filtering		TCP	80	80		
Everyday	IP Filtering		TCP	1	65535		

☐ Select All

Figure 8-14 Access Rule List - Example 3 (Continue)

Access Rule List							3/100
1/1	First	Prev	Next	Last	Go to Page	Search	
Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit	
	53	0.0.0.0	0.0.0.0	1	65535		
	80	0.0.0.0	0.0.0.0	1	65535		
	65535	0.0.0.0	0.0.0.0	1	65535		

☐ Select All

Figure 8-15 Access Rule List - Example 3 (Continue)

8.1.4.4 Example 4 - Control Internet Behaviors of a Single User

You can assign a range of contiguous IP addresses to the users that have the same Internet access privileges, and then create access rules for the user group. However, if one or several users in the group have special or new Internet needs, you need to individually create access rules for a single user.

In this example, we want to allow a group of users (IP address range: 192.168.1.10-192.168.1.120) to access web service, and block them from accessing all other services. The exception is that the user with IP address 192.168.1.16 is allowed to access all Internet services during business hours (Monday to Friday, 9:00 to 17:00).

We need to create four access rules to meet the requirements:

- Access rule 1: It allows the user group to access DNS service.
- Access rule 2: It allows the user group to access web service.
- Access rule 3: It allows the user with IP address 192.168.1.16 to access all Internet services during business hours.
- Access rule 4: It blocks the user group from accessing any Internet services.

Therein, rule 4 must have a lower priority than the other three rules.

Access Rule List

4/100

1/1FirstPrevNextLastGo toPage

Search

	Name	Status	Source IP Range	Priority	Action	Schedule	Filter
☐	Rule-1	Enabled	192.168.1.10--192.168.1.20	5	Allow	Everyday	IF
☐	Rule-2	Enabled	192.168.1.10--192.168.1.20	6	Allow	Everyday	IF
☐	Rule-3	Enabled	192.168.1.16--192.168.1.16	7	Allow	Mon,Tue,Wed,Thu,Fri;09:00-17:00	IF
☐	Rule-4	Enabled	192.168.1.10--192.168.1.20	8	Deny	Everyday	IF

☐ Select All

Add

Delete All

Delete

8.2 Domain Filtering

This section describes the **Firewall > Domain Filtering** page. The domain filtering feature allows you to block access to unwanted websites in your organization.

8.2.1 Domain Filtering Global Settings



Figure 8-19 Domain Filtering Global Settings

- ◆ **Enable Domain Filtering:** It allows you to enable or disable domain filtering. If you select the check box to enable domain filtering, the domain names in the **Domain Name List** will take effect. Else, they will be of no effect.
- ▶ **Save:** Click to save your changes.

8.2.2 Domain Filtering Settings



Figure 8-20 Domain Filtering Settings

- ◆ **Domain Name:** It specifies the domain name of the website that you want to block.
- ◆ **Domain Name List:** It displays the domain names that you have added. The Gigabit

Router will block the LAN users from accessing these domain names.

- ▶ **Add a Domain Name:** To add a domain name to the **Domain Name List**, enter the domain name of the website that you want to block in the **Domain Name** text box, and then click the **Add** button. You can add up to 100 domain names in the list.
- ▶ **Delete:** To delete one or more domain names, select them in the **Domain Name List**, and then click the **Delete** button.
- ▶ **Delete All:** To delete all the domain names in the **Domain Name List** at a time, directly click the **Delete All** button.



Note

1. The Gigabit Router supports up to 100 domain names.
2. The matching rule of domain filtering is whole words matching, that is, only a domain name matches the whole words of the domain name in the **Domain Name List**, the Gigabit Router will block access to it.
3. You can use the wildcard "*" in a domain name to filter multiple URLs. For example, if you add [www.163.*](http://www.163.com) into the **Domain Name List**, then all the URLs that begin with [www.163.](http://www.163.com) will be blocked.

8.3 Attack Prevention

This section describes the **Firewall > Attack Prevention** page.



Figure 8-21 Attack Prevention Settings

- ◆ **Enable DDoS Prevention:** It is used to enable or disable DDoS prevention. If you select the check box to enable this feature, it will effectively protect the Gigabit Router against popular DoS/DDoS attacks.
- ◆ **Enable Blaster Prevention** It is used to enable or disable blaster virus prevention. If you select the check box to enable this feature, it will effectively protect the Gigabit Router against popular virus attacks such as Blaster and Sasser.
- ◆ **Block WAN Ping:** It is used to block or allow WAN ping. If you select the check box to block WAN ping, all the WAN interfaces of the Gigabit Router will not respond to ping requests from the Internet.
- ▶ **Save:** Click to save your changes.

Chapter 9 VPN

The Gigabit Router supports PPTP client feature. PPTP is a VPN tunneling protocol which encapsulates PPP frames in IP packets for transmission over a public IP network such as the Internet. PPTP is based on client/server model. The PPTP client initiates a PPTP connection to the server, while the PPTP server accepts the incoming PPTP connection from the client. PPTP is often used to implement remote access VPNs over an IP network (such as a broadband network), to extend the reach of your Intranet.

9.1 Introduction to PPTP Implementation

PPTP is used to encapsulate PPP frames in IP packets for transmission over a public IP network such as the Internet. The PPTP client or server encapsulates the original user packets inside PPP frames before sending them through a PPTP tunnel over the Internet; while the peer performs decapsulation firstly, and then forward the original packets to their intended destinations.

As shown in Figure 9-1, the typical application of PPTP is that some laptop or desktop computers act as the PPTP client devices, that is, some employees in the remote branch offices or mobile users (traveling employees, telecommuters, etc.) use the Windows built-in PPTP client software to initiate PPTP connections; the PPTP server deployed at the head office accepts the PPTP incoming connections from the clients. After a PPTP tunnel has been established between the PPTP client and server, the PPTP server will receive the PPTP packets from the client firstly, and then perform decapsulation, lastly forward the original packets to their intended destinations.

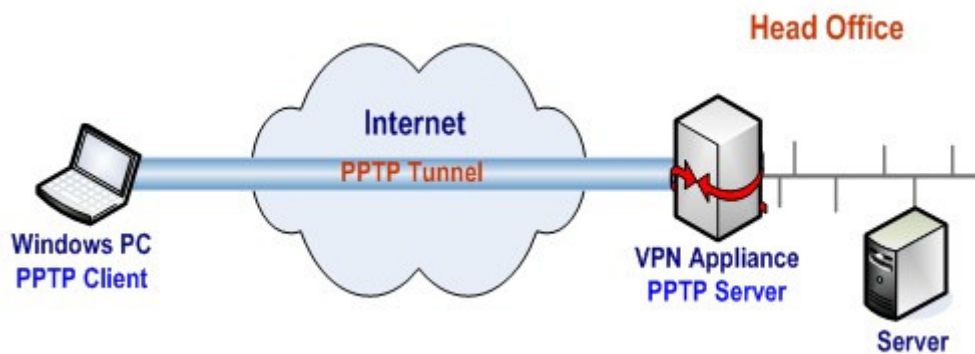


Figure 9-1 Typical Application of PPTP

9.1.1 Protocol Overview

There are two parallel components of PPTP:

1. A PPTP Control Connection

It is a logical connection representing the PPTP tunnel that must be created, maintained, and terminated through a series of PPTP messages. The PPTP control connection traffic uses a dynamically allocated TCP port on the PPTP client and the registered TCP port 1723 on the PPTP server.

2. GRE encapsulation for data

When data is sent through the PPTP tunnel, PPP frames are encapsulated with a Generic Routing Encapsulation (GRE) header, which includes information that identifies the specific PPTP tunnel for the data packet. GRE is described in RFC 1701.

The use of a separate GRE mechanism for PPTP data encapsulation has an interesting side effect for NAT devices. Most NAT devices can translate TCP-based packets for PPTP tunnel maintenance. However, many NAT devices or firewalls cannot handle GRE packets, thus the PPTP data packets with the GRE header cannot pass them. The UTT products support NAT traversal for PPTP tunnels.

In order for the PPTP tunnel to be established and function properly, the following basic conditions are necessary:

- 1) The PPTP client and server should have IP-route reachability between them.
- 2) The firewalls between the two endpoints of the tunnel should be configured to open TCP port 1723 and IP protocol 47 (GRE) to allow PPTP traffic.

9.1.2 Packet Flow - PPTP Client

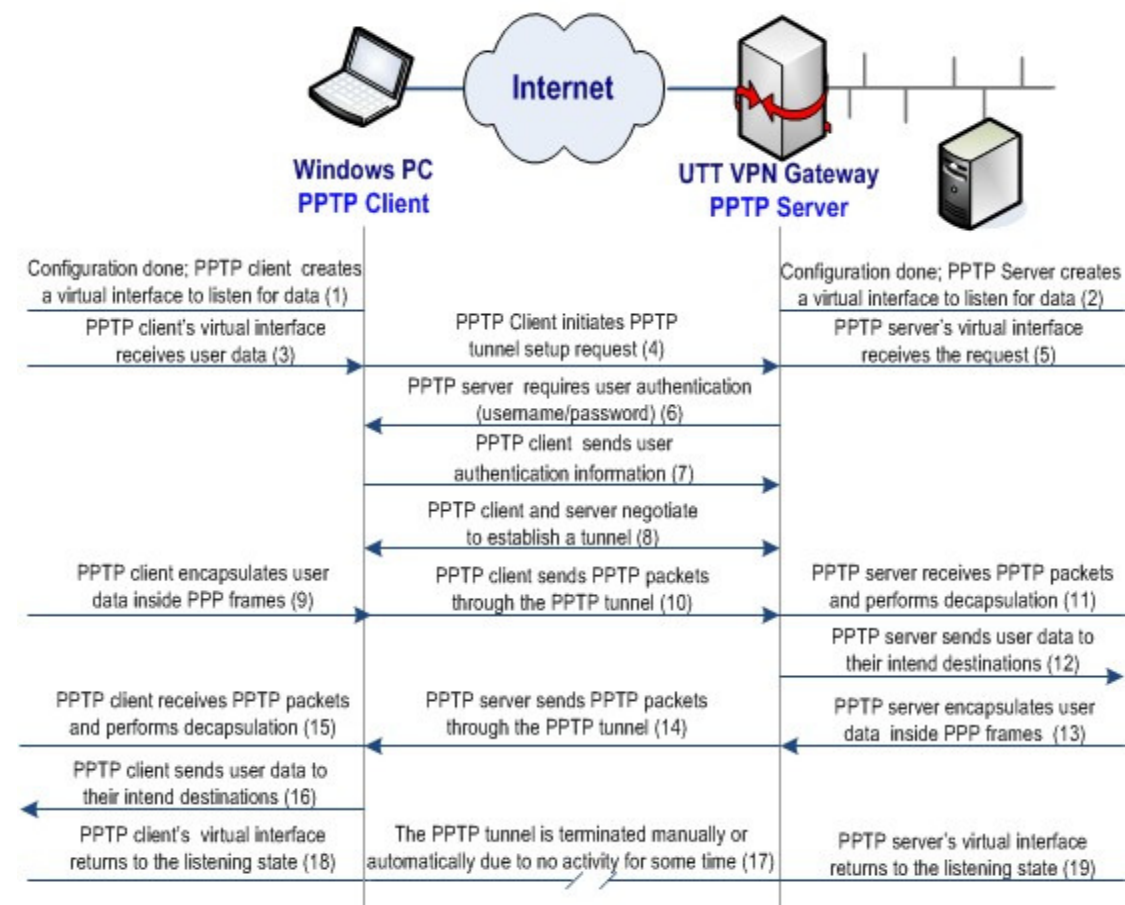


Figure 9-2 PPTP Packet Flow

As shown in Figure 9-2, during the PPTP tunnel establishment and data transmission processes, the packet flow through the PPTP client can be summarized as follows:

- After the PPTP tunnel parameters are configured properly, the PPTP client automatically creates a virtual interface for the new tunnel to listen for user data ((1) in Figure 9-2).
- The PPTP client's virtual interface listens for the user packets destined for the remote LAN ((3) in Figure 9-2).
- The PPTP client initiates the PPTP tunnel setup request ((4) in Figure 9-2).
- The PPTP client receives the user authentication request from the PPTP server, and then responds to the request ((7) in Figure 9-2).
- The PPTP client negotiates with the PPTP server to establish a PPTP tunnel ((8) in Figure 9-2).
- The PPTP client receives the user data (i.e., original packets) and encapsulates them in the PPP frames ((9) in Figure 9-2).

- The PPTP client sends the PPTP packets to the PPTP server through the PPTP tunnel ((10) in Figure 9-2).
- The PPTP client receives the PPTP packets from the PPTP server, and performs decapsulation ((15) in Figure 9-2).
- The PPTP client forwards the user data (i.e., original packets) to their intended destinations ((16) in Figure 9-2).
- The PPTP tunnel is terminated manually by the user or automatically due to no activity for some time ((17) in Figure 9-2).
- After the PPTP tunnel is terminated, the PPTP client's virtual interface returns to the listening state ((18) in Figure 9-2).

9.1.3 User Authentication

PPTP provides user authentication to authenticate the user attempting the PPTP connection by PPP-based user authentication modes such as PAP, CHAP, etc. Note that the two endpoints of a PPTP tunnel should use the same authentication mode.

On the Gigabit Router, it allows you to choose PAP, CHAP or Either as the user authentication mode for a PPTP client. It also allows you to choose None, which means that no authentication is performed. By default, the authentication mode is Either, which means that the PPTP client will automatically negotiate it with peer.

9.1.4 Data Confidentiality

PPTP doesn't provide any data encryption service by itself; it uses PPP compression and encryption mechanisms (such as CCP, PPE, etc.) to provide data confidentiality.

9.1.5 MTU and Fragmentation

The Gigabit Router will fragment an IP packet if it exceeds the MTU of the outbound physical interface. For example, a standard Ethernet-type interface has a MTU of 1500 bytes, thus the Gigabit Router will fragment a packet exceeding 1500 bytes in order to transmit it over the Ethernet interface.

With PPTP, the addition of PPTP headers may cause IP fragmentation. When an IP packet is nearly the size of MTU of the outbound physical interface (for example, ERP or FTP packets are often relatively large), and it is further encapsulated with PPTP headers,

the encapsulated packet is likely to exceed the MTU of the outbound physical interface. This causes the encapsulated packet to be fragmented before transmission, and the PPTP receiver is responsible for reassembling the fragments back into the original encapsulated packet before decapsulation. More specifically, the receiver cannot perform reassembly until the last fragment is received; and if one fragment is lost, the entire original encapsulated packet must be resent, and it will also be fragmented.

Data fragmentation and reassembly can seriously degrade the system performance, so it is highly necessary to avoid fragmentation and reassembly in the PPTP switching path. To solve this problem, PPTP allows the client and server to negotiate PPP MRU/MTU during PPTP tunnel establishment.

In addition, on the Gigabit Router, you can adjust the global PPTP tunnel MTU (i.e., tunnelmtu) to minimize the fragmentation: if an IP packet exceeds the specified MTU, it will be fragmented by the original computer before transmission. The following two examples describe how to calculate PPTP tunnel MTU. Figure 9-3 illustrates the format of the PPTP packet to be sent over a static IP or DHCP Internet connection; and Figure 9-4 illustrates the format of the PPTP packet to be sent over a PPPoE Internet connection. Therein, the sizes of standard Ethernet MTU and each encapsulation header are as follows:

Ethernet MTU	1500 Bytes
IP Header	20 Bytes
GRE Header	8 Bytes
PPTP Header	30 Bytes (at most)
PPPoE Header	8 Bytes



Figure 9-3 PPTP Packet Format - Static IP/DHCP Internet Connection

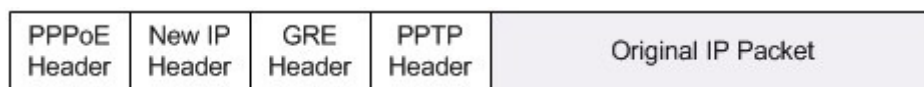


Figure 9-4 PPTP Packet Format - PPPoE Internet Connection

Therefore, to avoid fragmentation and reassembly in the PPTP switching path, the PPTP tunnel MTU should be smaller or equal to 1442 bytes ($1500 - 20 - 8 - 30 = 1442$) when the PPTP packets are sent over a static IP or DHCP Internet connection (see Figure 9-3); and it must be smaller or equal to 1434 bytes ($1442 - 8 = 1434$) when the PPTP packets are sent over a PPPoE Internet connection (see Figure 9-4).

On the Gigabit Router, the PPTP tunnel MTU is 1400 bytes by default. In most cases, please leave the default value because it can meet most application needs.

9.1.6 PPTP Sessions Limit

The Gigabit Router supports two concurrent PPTP sessions (i.e., tunnels) at most. If there are already two active PPTP sessions on the Gigabit Router, the system will reject any request for creating a new PPTP session and prompt you.

9.2 PPTP Client Settings

Enable ☒

Tunnel Name * tunnel-1

User Name * test

Password * ••••••

PPP Authentication Either ▼

Remote Subnet IP * 192.168.16.1

Remote Subnet Mask * 255.255.255.0

Tunnel Server IP/Domain Name * 200.200.200.251

Save Cancel Back

Figure 9-5 PPTP Client Settings

- ◆ **Enable:** It allows you to enable or disable the PPTP client entry. The default value is checked, which means the PPTP client entry is in effect. If you want to disable the entry temporarily instead of deleting it, please clear the check box.
- ◆ **Tunnel Name:** It specifies a unique name of the PPTP tunnel. It is used to identify multiple tunnels.
- ◆ **User Name:** It specifies a unique user name of the PPTP/L2TP client. It must be between 1 and 31 characters long. The remote PPTP/L2TP server will use the **User Name** and **Password** to identify the client.
- ◆ **Password:** It specifies a password of the PPTP/L2TP client.
- ◆ **PPP Authentication:** It specifies the PPP authentication mode by which the remote PPTP server authenticates the PPTP client. The available options are **None**, **PAP**, **CHAP** and **Either**.
 - **PAP:** Password Authentication Protocol.
 - **CHAP:** Challenge Handshake Authentication Protocol.

- **None:** It means that no authentication is performed.
- **Either:** It means that the Gigabit Router will automatically negotiate it with the remote VPN appliance.
- ◆ **Remote Subnet IP:** It specifies the subnet IP address of the remote network. In most cases, you may enter the IP address of the remote VPN appliance's LAN interface.
- ◆ **Remote Subnet Mask:** It specifies the subnet mask of the remote network.
- ◆ **Tunnel Server IP/Domain Name:** It specifies the IP address or domain name of the remote PPTP/L2TP server. In most cases, you may enter the WAN IP address or domain name of the remote VPN appliance.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **PPTP Client List**.

9.3 PPTP Client List

After you have configured a PPTP/L2TP client entry, you can view its configuration and status in the **PPTP Client List**, see Figure 9-6.

The screenshot shows the 'PPTP Client List' interface. At the top, there's a header 'PPTP Client List' and a page indicator '1/2'. Below the header is a navigation bar with links: '1/1', 'First', 'Prev', 'Next', 'Last', 'Go to Page', and a search box. The main table has columns: Tunnel Name, User Name, Enabled, Remote Subnet IP, Remote Subnet Mask, Status, Up Time, and Out Bytes. There is one row with the following data: Tunnel Name: 'tunnel-1', User Name: 'test', Enabled: 'Yes', Remote Subnet IP: '192.168.16.0', Remote Subnet Mask: '255.255.255.0', Status: 'Disconnected', Up Time: '-', and Out Bytes: '-'. Below the table is a scroll bar and a set of buttons: 'Add', 'Delete', 'Connect', 'Disconnect', and 'Refresh'.

Tunnel Name	User Name	Enabled	Remote Subnet IP	Remote Subnet Mask	Status	Up Time	Out Bytes
tunnel-1	test	Yes	192.168.16.0	255.255.255.0	Disconnected	-	-

Figure 9-6 PPTP Client List

This screenshot is a continuation of the previous one, showing the same 'PPTP Client List' interface. The table now includes an 'Edit' column with a pencil icon for the 'test' user. The buttons at the bottom remain the same: 'Add', 'Delete', 'Connect', 'Disconnect', and 'Refresh'.

Tunnel Name	Enabled	Remote Subnet IP	Remote Subnet Mask	Status	Up Time	Out Bytes	In Bytes	Edit
test	Yes	192.168.16.0	255.255.255.0	Disconnected	-	-	-	

Figure 9-7 PPTP Client List (Continue)

After the Gigabit Router has successfully established a PPTP tunnel with the remote

PPTP server, you will see that the tunnel's **Status** changes from **Disconnected** to **Connected**, the **Up Time** timer starts, and the **Out Bytes** and **In Bytes** will go on increasing as long as there is some network traffic being passed through the PPTP tunnel.

9.4 Configuration Example for PPTP Client

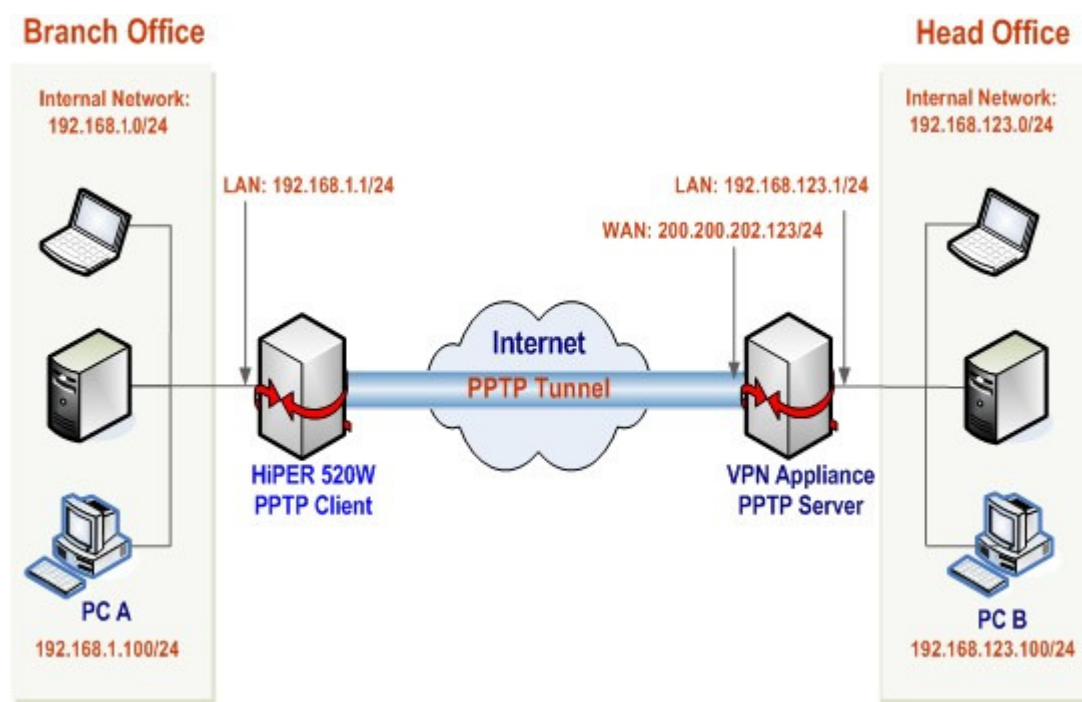


Figure 9-8 Network Topology - The Gigabit Router Acts as a PPTP client

In this example, a company's head office is located in Washington, and its branch office is located in New York. Now the company wants the head office and branch office to securely communicate with each other over the Internet.

As shown in Figure 9-8, we will use PPTP to establish a VPN tunnel, deploy a HiPER 840G Gigabit Router acting as a PPTP client at the branch office, and another VPN appliance (a UTT VPN gateway is recommended) acting as a PPTP server at the head office. The IP addresses are as follows:

The HiPER 840G (PPTP Client) at the branch office:

- LAN Subnet: 192.168.1.0/255.255.255.0
- LAN Interface IP Address: 192.168.1.1/255.255.255.0

The VPN appliance (PPTP Server) at the head office:

- LAN Subnet: 192.168.123.0/255.255.255.0
- LAN Interface IP Address: 192.168.123.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.123/255.255.255.0

To configure the HiPER 840G as a PPTP client, follow these steps:

Step 1 Go to the **VPN > PPTP Client** page, and click the **Add** button to go to the **PPTP Client Settings** page.

Step 2 Make the following settings.

Enable	Select
Tunnel Name	To_HQ
User Name	VPN_test
Password	vpntest
PPP Authentication	Either
Remote Subnet IP	192.168.123.1
Remote Subnet Mask	255.255.255.0
Tunnel Server IP/Domain Name	200.200.202.123

Step 3 Click the **Save** button.

9.5 IPSec VPN

With the development of network safety standards and protocols, various VPN technologies have emerged. IPSec VPN is one of the most widely used VPN security technologies today.

IPSec is a set of open standards and protocols to implement network secure communication, which provides two security mechanisms: encryption and authentication. Encryption mechanism is used to ensure data confidentiality; and authentication mechanism is used to ensure that data is from the claimed sender and not destroyed or tampered during transmission.

9.5.1 Introduction to IPSec Implementation

As shown in **Table 11-1 Four Types of IPSec VPN Configuration**, the UTT VPN gateway supports four types of IPSec VPN configuration.

ID	Key Mode	Connection Type	P1 Exchange Mode
----	----------	-----------------	------------------

Utt Technologies		Chapter 10 VPN	
1	Manual Key	Gateway-to-Gateway IPSec VPN	

2	AutoKey (IKE)	Bidirectional (Gateway-to-Gateway IPSec VPN)	Main Mode
3	AutoKey (IKE)	Originate-Only (Dynamic-to-Static IPSec VPN)	Aggressive Mode
4	AutoKey (IKE)	Answer-Only (Static-to-Dynamic IPSec VPN)	Aggressive Mode

Table 11-1 Four Types of IPSec VPN Configuration

In the first and second types of IPSec VPN configuration, both IPSec endpoints have static IP addresses; in the third type, the local UTT VPN gateway has a dynamic IP address, while the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a static IP address; and in the last type, the local UTT VPN gateway has a static IP address, while the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a dynamic IP address. In addition, on the local UTT VPN gateway, you can specify a Fully Qualified Domain Name (FQDN) instead of an IP address for the remote IPSec endpoint (another UTT VPN gateway or compatible VPN appliance that supports DDNS) with a dynamic IP address; this means that you can establish an IPSec tunnel between two endpoints that both have dynamic IP addresses.

9.5.1.1 Concepts and Protocols

In order for the IPSec tunnel to be established and function properly, the two IPSec endpoints must agree on the SAs. The IPSec SAs determine a number of security parameters (like security protocol, security algorithms and keys, SA lifetime, etc.) necessary to secure and maintain the IPSec tunnel effectively. An SA is uniquely identified by three parameters: security parameters index (SPI), destination IP address, and security protocol (AH or ESP).

Through the SAs, an IPSec tunnel can provide any combination of the following types of protection:

- **Data Confidentiality:** The IPSec sender can encrypt datagrams before transmitting them, and only the IPSec receiver can decrypt and read them.
- **Data Integrity:** The IPSec receiver can verify that the datagram is not altered during transmission, either deliberately or due to random errors.
- **Data Origin Authentication:** The IPSec receiver can verify that each datagram is originated by the claimed sender.
- **Anti-Replay:** The IPSec receiver can detect and reject replayed packets (i.e., old or duplicate packets) to prevent replay attacks.

IPSec provides two security protocols including AH and ESP for protecting data. AH is used to provide data authentication service (data origin authentication and data integrity).

ESP is used to provide data encryption and/or data authentication service. To use an IPSec tunnel to protect your data, you can choose different security policies as required.

You can choose AH or ESP to provide authentication service only, or choose ESP to provide encryption service only. Of course, you can choose ESP together with AH or only ESP to provide both authentication and encryption services for your data. With IPSec, most network security designers will choose to provide all of the supported security services, including data confidentiality, data integrity, data origin authentication, and anti-replay, for the data, which are currently the highest level of data protection services in the IP network.

The IPSec architecture is shown in **Figure 11-11 IPSec Architecture**.

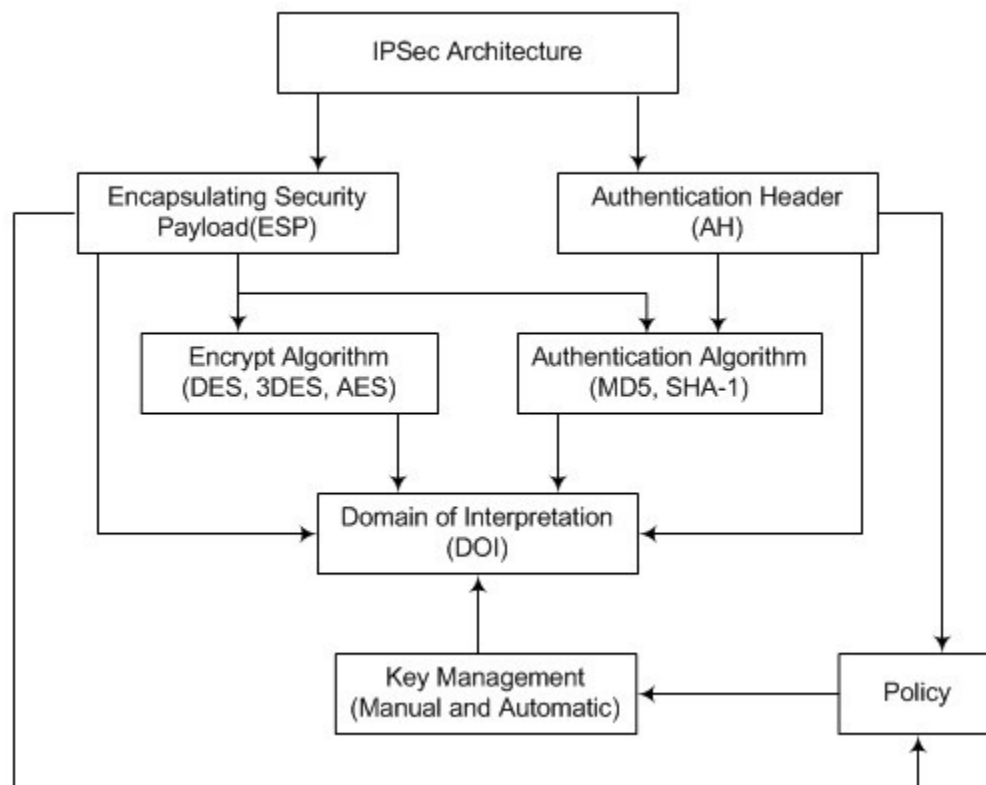


Figure 11-11 IPSec Architecture

IPSec supports two methods to create security associations (SAs):

- The SAs can be created manually by the system administrator, which is called **Manual Key** on the UTT VPN gateway;
- The SAs can be negotiated and created dynamically by IKE, which is called **AutoKey (IKE)** on the UTT VPN gateway.

9.5.1.2 IPSec Modes

IPSec has two basic modes of operation: transport mode and tunnel mode. In transport

mode, only the original IP packet's payload is protected. In tunnel mode, the entire original IP packet is protected and then encapsulated into a new IP packet.

When both endpoints of an IPSec tunnel are hosts, you can use transport mode or tunnel mode. When either end of the tunnel is a security gateway (such as a router or firewall), or both ends are security gateways, you must use tunnel mode. On the UTT VPN gateway, IPSec always operates in tunnel mode.

1. Tunnel Mode

In tunnel mode, the entire original IP packet including IP header and payload is protected and then encapsulated into a new IP packet. As shown in **Figure 11-12 Tunnel Mode**, the IPSec AH and/or ESP header is appended to the front of the original IP header, and then a new IP header is appended to the front of the IPSec header. The source and destination IP addresses in the new IP header are those of the two endpoints of the IPSec tunnel respectively.

The entire original IP packet can be encrypted, authenticated, or both. With AH, the AH and new IP headers can also be authenticated. With ESP, the ESP header can also be authenticated, but the new IP header cannot be authenticated.

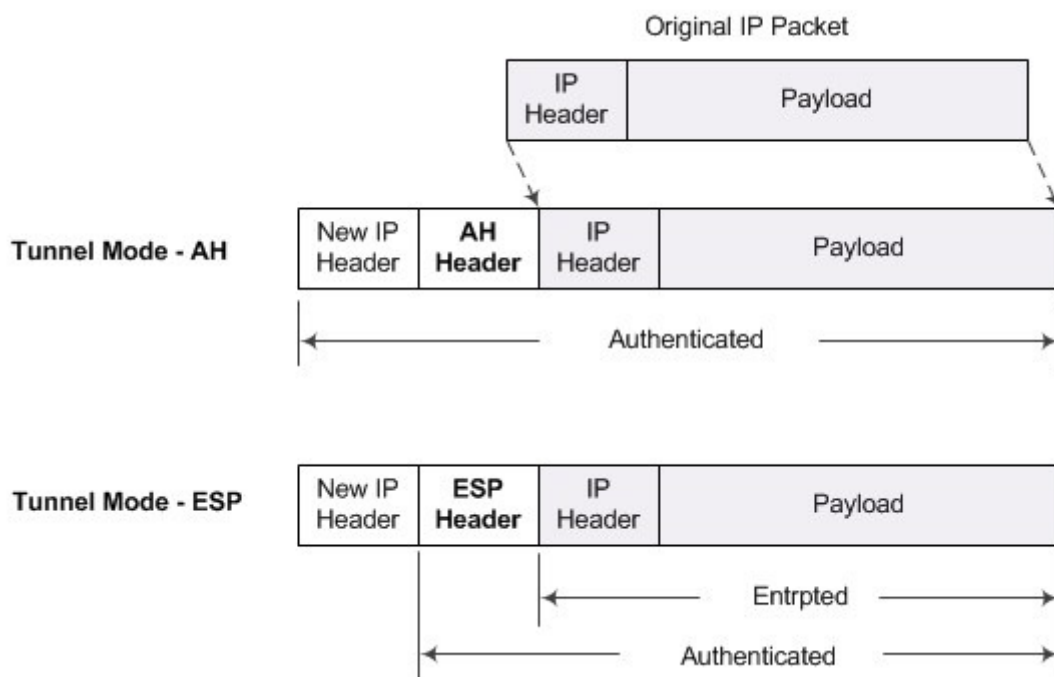


Figure 11-12 Tunnel Mode

2. Transport Mode

In transport mode, only the original IP packet's payload is protected. As shown in **Figure 11-13 Transport Mode**, the IPSec AH and/or ESP header is appended to the front of the payload. With AH, the entire IP packet can be authenticated. With ESP, the payload can be encrypted and authenticated, and the ESP header also can be authenticated, but the

original IP header cannot be authenticated.

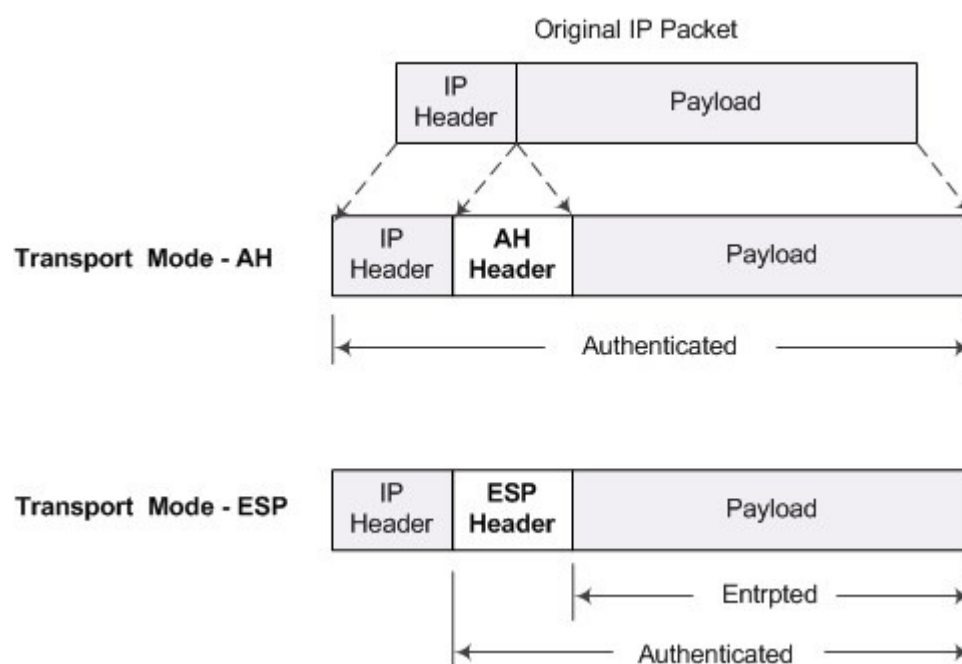


Figure 11-13 Transport Mode

9.5.1.3 Key Management

The term **key management** refers to the creation, distribution, storage and deletion of keys. Key management is a critical part of IPSec. IPSec uses cryptographic keys for authentication and encryption. On the UTT VPN gateway, IPSec supports both manual and automatic key management.

1. Manual Key

With manual key management, all the security parameters at both endpoints of an IPSec tunnel are configured manually. In general, there are more than 20 parameters that need to be configured at each endpoint.

Manual key management is feasible for small VPN networks (such as, a network with a few VPN appliances) where the distribution, maintenance and tracking of keys are not difficult. However, for large VPN networks with a large number of VPN appliances across great distances, this method is often unreliable or infeasible. When a key is initially distributed, there may be no way to verify that the key has not been compromised during transmission. In addition, whenever you want to change the keys, you need redistribute the new keys to all the VPN appliances; and this causes the same security issues as when the key was initially distributed. In conclusion, manual key management is only suitable for relatively small VPN networks.

2. AutoKey (IKE)

To improve security and lessen the burden on administrators, IPSec supports Internet Key Exchange (IKE) protocol. Using IKE protocol, the two IPSec endpoints can automatically generate and negotiate keys and security associations. This automatic key management method is called **AutoKey (IKE)** on the UTT VPN gateway.

At present the UTT VPN gateway supports AutoKey (IKE) based on preshared keys. The preshared key is used as a seed key to generate IPSec session keys. Both IPSec endpoints should have the same preshared key. With **AutoKey (IKE)** management, the key distribution is the same as that with manual key management. However, once distributed, the two endpoints (unlike manual key) will automatically change their session keys at the specified time interval using IKE protocol. This is done without human intervention; therefore, using **AutoKey (IKE)** method can also reduce management cost and burden.

Often changing keys enhance security. However, changing keys increases traffic overhead; therefore, to avoid reducing data transmission efficiency, it is suggested that you do not choose to change keys too often.

9.5.1.4 Creating Security Associations (SAs)

The concept of a Security Association (SA) is fundamental to IPSec. An SA is a relationship between two IPSec endpoints that describes how the endpoints will use security services to communicate. Each SA consists of a set of security parameters like security protocol (ESP or AH), encryption and/or authentication algorithms, session keys, SA lifetime, and so on. Because an IPSec SA is simplex (unidirectional) in nature, a bidirectional communication requires at least two SAs, one in each direction.

In **Manual Key** mode, negotiations are not required because all the necessary SA parameters are defined during the configuration of the IPSec tunnel. In this case, if the UTT VPN gateway receives a packet matching an IPSec security policy, it will encrypt and authenticate the packet, and then send it to the remote endpoint through the IPSec tunnel.

In **AutoKey (IKE)** mode, the basic operation of IKE can be broken down into two phases:

- IKE Phase 1 is used to authenticate the two endpoints and negotiate the parameters and key material required to establish a secure channel (i.e., IKE SA). The IKE SA is then used to protect further IKE exchanges.
- IKE Phase 2 is used to negotiate the parameters and key material required to establish IPSec SAs. The IPSec SAs are then used to authenticate and encrypt the user data.

1. IKE Phase 1

During IKE phase 1, one or more security proposals are exchanged and agreed upon

between the two endpoints. The two endpoints exchange proposals for acceptable security services such as:

- Encryption algorithm (DES, 3DES, or AES 128/192/256)
- Authentication algorithm (MD5 or SHA-1)
- Diffie-Hellman group (Refer to **Diffie-Hellman Exchange** described later in this section for more information.)
- Preshared key

When both IPSec endpoints agree to accept at least one set of the proposed phase 1 security parameters and then process them, a successful phase 1 negotiation concludes. When acting as an initiator, the UTT VPN gateway supports up to 12 phase 1 proposals, which allow you to specify a series of security parameters; when acting as a responder, it can accept any phase 1 proposal.

By default, the UTT VPN gateway provides four phase 1 proposals, which include:

- 3des-md5-group2
- 3des-sha-group2
- des-md5-group2
- des-sha-group2

It also allows you to specify phase 1 proposals as required.

*In the Web UI, it allows you to configure up to four phase 1 proposals. You can go to the **VPN > IPSec > IPSec Settings** page to configure the **Preshared Key**, and then click the **Advanced Options** hyperlink to configure **Encrypt/Auth Algorithms 1 ~ Encrypt/Auth Algorithms 4 (Phase 1)** (section 6.1.2.2).*

➤ Main Mode and Aggressive Mode

IKE supports two modes of its phase 1 negotiations: main mode and aggressive mode, the following describes them respectively.

Main Mode

Main mode has three two-way exchanges with a total of six messages between the initiator and the responder.

- First exchange (message 1 and 2): The encryption and authentication algorithms used to secure the IKE communications are negotiated and agreed upon between the two endpoints.

- Second exchange (message 3 and 4): A Diffie-Hellman exchange is performed. Each endpoint exchanges a nonce (i.e., random number).
- Third exchange (message 5 and 6): Identities of both endpoints are exchanged and verified.

In the third exchange, identities are not transmitted in clear text. The identities are protected by the encryption algorithm agreed upon in the first two exchanges.

*In the Web UI, you can go to the **VPN > IPSec > IPSec Settings** page to click the **Advanced Options** hyperlink to select **Main** from the **Exchange Mode** drop-down list (section 6.1.2.2).*

Aggressive Mode

Aggressive mode has two exchanges with a total of three messages between the initiator and the responder.

- First message: The initiator proposes the SA, initiates a Diffie-Hellman exchange, and sends a nonce (i.e., random number) and its IKE identity.
- Second message: The responder accepts the proposed SA, authenticates the initiator, and sends a nonce (i.e., random number), its IKE identity, and its certificates if it is being used.
- Third message: The initiator authenticates the responder, confirms the exchange, and sends its certificates if it is being used.

The weakness of using aggressive mode is that it does not provide identity protection

because the identities of both sides are exchanged in clear text. However, aggressive

mode is faster than main mode.

*In the Web UI, you can go to the **VPN > IPSec > IPSec Settings** page to click the **Advanced Options** hyperlink to select **Aggressive** from the **Exchange Mode** drop-down list (section 6.1.2.2).*



Note

If one of the two IPSec endpoints has a dynamic IP address, you must use aggressive mode to establish an IPSec tunnel.

➤ Diffie-Hellman Exchange

The Diffie-Hellman exchange is a public key cryptography protocol used for key exchange. With Diffie-Hellman exchange, the two IPSec endpoints publicly exchange key material over an insecure network channel to derive a shared secret key, which is never exchanged over the insecure channel.

There are five basic DH groups (UTT VPN gateway supports DH groups 1, 2, and 5). Each DH group has a different size modulus. A larger modulus provides higher security, but requires more processing time to generate the key. The modulus of DH groups 1, 2, and 5 are as follows:

- DH Group 1: 768-bit modulus
- DH Group 2: 1024-bit modulus
- DH Group 5: 1536-bit modulus

**Note**

Both endpoints of an IPSec tunnel should use the same DH group because each group has a different size modulus.

*In the Web UI, you can go to the **VPN > IPSec > IPSec Settings** page to click the **Advanced Options** hyperlink to select DH groups by **Encrypt/Auth Algorithms 1 ~ Encrypt/Auth Algorithms 4 (Phase 1)** (section 6.1.2.2).*

2. IKE Phase 2

Once an IKE SA is established successfully in phase 1, the two IPSec endpoints will use it to negotiate IPsec SAs in phase 2. The IPsec SAs are used to secure the user data to be transmitted through the IPSec tunnel.

During IKE Phase 2, the two IPSec endpoints also exchange security proposals to determine which security parameters to be used in the IPsec SAs. A phase 2 proposal consists of one or two IPsec security protocols (either ESP or AH, or both), the encryption and/or authentication algorithms used with the selected security protocol, and a Diffie-Hellman if Perfect Forward Secrecy (PFS) is desired. Note that the UTT VPN gateway doesn't support PFS at present.

IKE phase 2 has one mode, which is called **Quick Mode**. Quick mode uses three messages to establish IPsec SAs.

*In the Web UI, it allows you to configure up to four phase 2 proposals. You can go to the **VPN > IPSec > IPSec Settings** page to configure **P2 Encrypt/Auth Algorithms 1**, and then click the **Advanced Options** hyperlink to configure **Encrypt/Auth Algorithms 2 ~ Encrypt/Auth Algorithms 4 (Phase 2)** (section 6.1.2.2).*

9.5.1.5 Maintain Security Associations (SAs)

After the SAs have been established, the two IPSec endpoints should maintain the SAs to ensure that the SAs are secure and available. IPsec provides the following methods to maintain and detect SAs.

1. SA Lifetime

During IKE and IPsec SAs negotiation and creation, the two IPSec endpoints also

negotiate a lifetime for each SA. If an SA is nearing the end of the lifetime, the endpoints must negotiate and create a new SA and use it instead. The SA lifetime specifies how often each SA should be renegotiated, either based on elapsed time or the amount of network traffic.

*In the Web UI, you can go to the **VPN > IPSec > IPSec Settings** page to click the **Advanced Options** hyperlink to configure the lifetime of IKE SA by the parameter **Time Lifetime (Phase 1)**, and configure the lifetime of IPSec SAs by the parameters **Time Lifetime (Phase 2)** and **Data Lifetime (Phase 2)** (section 6.1.2.2).*

Reducing the lifetime forces the IPSec endpoints to renegotiate the SAs more frequently. This frequent renegotiation improves security, but at the expense of higher CPU utilization and possible delays during the renegotiation process. Therefore, the SA lifetime is often set to a relatively long time (the suggested value is between 1 and 24 hours). Because there is no way for the IPSec endpoints to identify the loss of peer connectivity, the SAs can remain until their lifetimes naturally expire, and each endpoint assumes that its peer is available before their SAs expire. Then, if the connectivity between the two endpoints goes down unexpectedly due to routing problems, system rebooting, etc., one endpoint still continues to send the packets to its peer until the SAs expire; this results in a false connection (SAs are normal, but the tunnel is disconnected) where packets are tunneled to oblivion. Therefore, it is necessary that either endpoint can detect a dead peer as soon as possible; a method called Dead Peer Detection (DPD) is used to achieve this purpose. DPD has smaller cost than SA renegotiation, so it is always performed at a higher frequency.

2. DPD (Dead Peer Detect)

Dead Peer Detection (DPD) is a traffic-based method of detecting a dead IKE peer. DPD allows an endpoint to prove its peer's liveliness periodically. This can help the endpoint to avoid a situation where it sends IPSec packets to a peer that is no longer available ("Martian" host). After DPD is enabled, the endpoint periodically sends DPD heartbeat messages at the specified time interval (usually 20 seconds or about 1 minute) to the peer to verify its availability. After missing several consecutive heartbeat messages, the endpoint will renegotiate the SAs with the peer.

*In the Web UI, you can go to the **VPN > IPSec > IPSec Settings** page to click the **Advanced Options** hyperlink to select the **DPD** check box to enable DPD feature, and configure the parameter **Heartbeat Interval** to specify a time interval at which the UTT VPN gateway periodically sends DPD heartbeat messages to the peer to verify its availability (section 6.1.2.2).*

9.5.1.6 IPSec Tunnel Establishment Process

When used in context with IPSec, the initiator refers to the IPSec endpoint that initiates IKE negotiation, and the responder refers to the IPSec endpoint that responds to incoming IKE request.

IPSec works in peer-to-peer mode, where either endpoint of an IPSec tunnel can act as

an initiator or a responder. However, for a dynamic-to-static or static-to-dynamic IPSec tunnel with IKE aggressive mode, the IPSec endpoint with a static IP address cannot initiate IKE negotiation because it doesn't know where to send request; therefore, it will only act as a responder, and the IPSec endpoint with a dynamic IP address will only act as an initiator.

On the UTT VPN gateway, IPSec tunnel implementation is based on security virtual interface, which is quite different from the PPTP virtual interface. The following describes the main differences between them.

1. Drive Mechanism

The PPTP virtual interface is driven by the routing table; and you cannot create different PPTP virtual interfaces based on service type. But the IPSec virtual interface is driven by the Security Policy Database (SPD); and you can create different virtual interfaces based on service type. For example, the UTT VPN gateway will forward the packets destined for the same destination network (such as a corporate network) through the same route; however, the UTT VPN gateway can be configured to encrypt some of them (such as email packets) by IPSec, but not encrypt others (such as http packets).

*In the Web UI, you can go to the **VPN > IPSec > IPSec Settings** page to click the **Advanced Options** hyperlink, and then configure the filter parameters including **Protocol** and **Port** to define the packets that are protected by IPSec (section 6.1.2.1 and 6.1.2.2).*

2. Creation Method

Once the PPTP tunnel parameters have been configured properly, the system will automatically create a virtual interface for the new tunnel to transmit data, and add two routes pointing to the virtual interface into the routing table (refer to section 2.2.2 and 3.2.2 for more information).

However, once the IPSec tunnel parameters have been configured properly, the system will automatically add the new security policy in the Security Policy Database (SPD). When the system receives an outbound packet, it will compare the packet against the SPD to find the first matching entry. If the first matching entry requires IPSec processing, the system will encrypt and/or authenticate the packet, and then sends it out. When the system receives an inbound packet, it will check the packet to see whether it contains an IPSec header; if not, the packet will be forwarded directly. Else, the UTT VPN gateway will authenticate and/or decrypt the packet, and then forward the resulting packet (i.e., initial packet) to its intend destination.

*In the CLI, you can use the **show crypt ipsec sp** command to check if the security policy is created. As shown in **Figure 11-14 Viewing IPSec Security Policy**, "found 1 items in eroute table" means that there is one security policy entry in the SPD now.*

```

profile if_n out_fi in_fi tunSrc tunDst H M
-----
PPPOE1 4 to_bj0 to_bj1 218.80.111.98 221.216.15.158 Y N

--More Detail--
out_fi mtu a_rly nat_t kp_alu udp_e dport dpd_hb dpd_to dpd_a
-----
to_bj0 1450 N Y 20 N 0 0 0 0
found 1 items in eroute table!

```

Figure 11-14 Viewing IPSec Security Policy

3. Trigger Way

The PPTP virtual interface is triggered by the IP route. However, the IPSec virtual interface is triggered by the security policy in the Security Policy Database (SPD). The IPSec module starts outbound packet processing after the IP module has processed the packet, and completes inbound packet processing before the IP module receives the packet. By changing the execution order of triggers, you can implement IPSec over PPTP or PPTP over IPSec on the gateway to provide the most powerful VPN functionality.

When the UTT VPN gateway receives an outbound packet that requires IPSec protection and the IPSec tunnel is not established, it will initiate IKE negotiation to establish a pair of IPSec SAs (that is, an IPSec tunnel). After the IPSec tunnel is established, the UTT VPN gateway will do the required IPSec processing (e.g., encryption and/or authentication) before sending the packet to the remote endpoint through the tunnel; and the remote endpoint will do the required IPSec processing (e.g., authentication and/or decryption) before sending the packet to its intend destination.

In the CLI, you can use the **show crypt ipsec sa** command to check if the IPSec tunnel is established.

As shown in **Figure 11-15 Viewing IPSec SAs**, “total: 1 SAs active” means that there is a pair of active SAs now, in other words, there is an IPSec tunnel established.

```

... ..
total: 1 SAs active!

```

Figure 11-15 Viewing IPSec SAs



Note

For a dynamic-to-static or static-to-dynamic IPSec tunnel with IKE aggressive mode, the IPSec endpoint with a static IP address cannot initiate IKE negotiation because it doesn't know where to send request; therefore, it will only act as a responder, and the IPSec endpoint with a dynamic IP address will only act as an initiator.

9.5.1.7 Packet Flow – IPSec Initiator

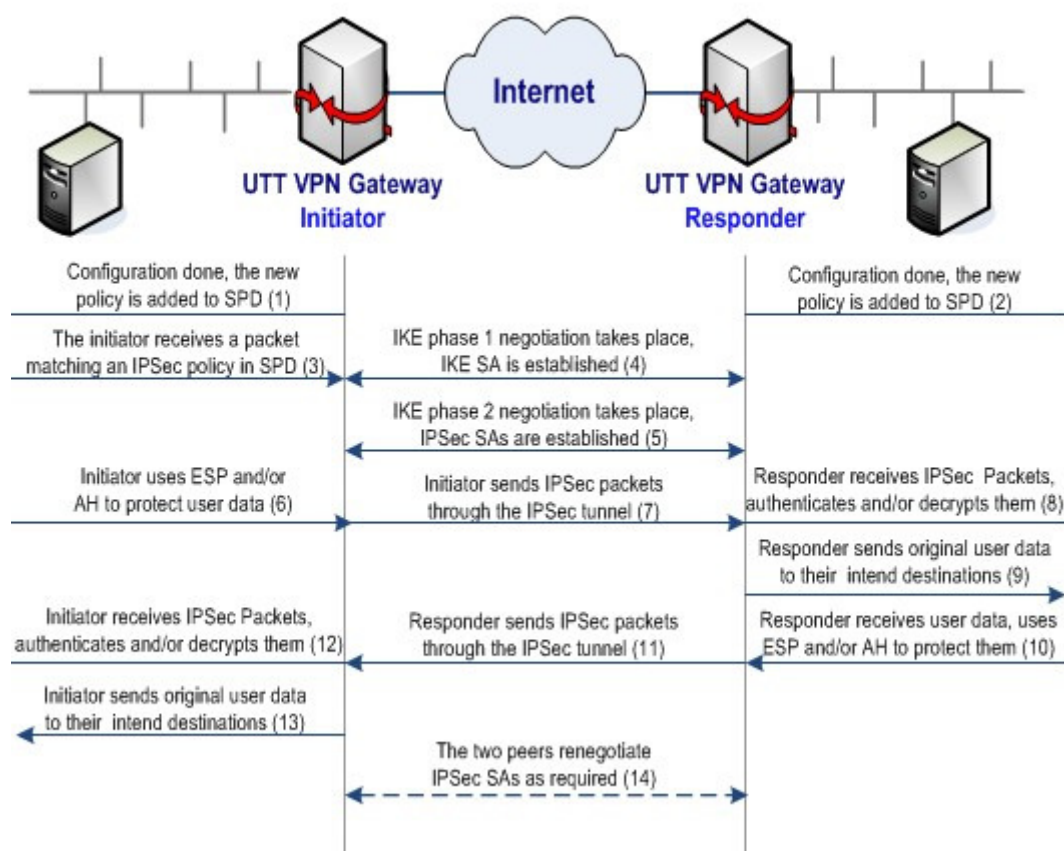


Figure 11-16 IPSec Packet Flow

As shown in **Figure 11-16 IPSec Packet Flow**, during the IPSec tunnel establishment and data transmission processes, the packet flow through the IPSec initiator can be summarized as follows:

1. After the IPSec tunnel parameters are configured properly, the new policy is added into the SPD (1) in.
2. The initiator receives a packet that matches an IPSec policy in the SPD (3) .
3. IKE phase 1 negotiation takes place (started by the initiator), and the IKE SA is established (4). Refer to section 4.2.1.3 for more information.
4. IKE phase 2 negotiation takes place, and the IPSec SAs are established (5) The initiator uses ESP and/or AH to protect the user data (i.e., original packets) (6)
5. The initiator sends the IPSec packets to the responder through the IPSec tunnel (7) The initiator receives the IPSec packets from the responder, and authenticates and/or decrypts them (12).
6. The initiator forwards the user data (i.e., original packets) to their intend destinations (13).
7. The two endpoints renegotiate IPSec SAs as required (14). Refer to section 4.2.1.4

for more information.

9.5.1.8 Packet Flow – IPSec Responder

As shown in **Figure 11-16 IPSec Packet Flow**, during the IPSec tunnel establishment and data transmission processes, the packet flow through the IPSec responder can be summarized as follows:

1. After the IPSec tunnel parameters are configured properly, the new policy is added into the SPD (2).
2. IKE phase 1 negotiation takes place (started by the initiator), and the IKE SA is established (4). Refer to section 4.2.1.3 for more information.
3. IKE phase 2 negotiation takes place, and the IPSec SAs are established (5).
4. The responder receives the IPSec protected packets from the initiator, and authenticates and/or decrypts them (8).
5. The responder forwards the user data (i.e., original packets) to their intend destinations (9).
6. The responder receives the user data (i.e., original packets), and then uses ESP and/or AH to protect them (10).
7. The responder sends the IPSec packets to the initiator through the IPSec tunnel (11)
8. The two endpoints renegotiate IPSec SAs as required (14). Refer to section 4.2.1.4 for more information.



Note

In **Manual Key** mode, IKE phase 1 and phase 2 negotiations are not required because all the necessary SA parameters are defined during the configuration of the IPSec tunnel.

9.5.1.9 MTU and Fragmentation

The UTT VPN gateway will fragment an IP packet if it exceeds the MTU of the outbound physical interface. For example, a standard Ethernet-type interface has a MTU of 1500 bytes, thus the UTT VPN gateway will fragment a packet exceeding 1500 bytes in order to transmit it over the Ethernet interface.

With IPSec, the addition of IPSec headers may cause IP fragmentation. When an IP packet is nearly the size of MTU of the outbound physical interface (for example, ERP or FTP packets are often relatively large), and it is further encapsulated with IPSec headers, the encapsulated packet is likely to exceed the MTU of the outbound physical interface. This causes the encapsulated packet to be fragmented before transmission, and the IPSec receiver is responsible for reassembling the fragments back into the original encapsulated packet before decapsulation (authentication and/or decryption). More specifically, the receiver cannot perform reassembly until the last fragment is received;

and if one fragment is lost, the entire original encapsulated packet must be resent, and it will also be fragmented.

Data fragmentation and reassembly can seriously degrade the system performance, so it is highly necessary to avoid fragmentation and reassembly in the IPsec switching path. To solve this problem, the UTT VPN gateway allows you to set the IPsec tunnel MTU to minimize the fragmentation. If an IP packet exceeds the specified MTU, it will be fragmented by the original host before transmission.

*In the CLI, you can use the **set ipsec config/xxx mtu** command to set the IPsec tunnel MTU.*

The Web UI doesn't support this function.

The following two examples describe how to calculate IPsec tunnel MTU in the case of tunnel mode. **Figure 11-17 IPsec Packet Format – Static IP/DHCP Internet Connection** illustrates the format of the IPsec packet to be sent over a static IP or DHCP Internet connection; and **Figure 11-18 IPsec Packet Format – PPPoE Internet Connection** illustrates the format of the IPsec packet to be sent over a PPPoE Internet connection. Therein, the sizes of standard Ethernet MTU and each encapsulation header are as follows:

Ethernet MTU	1500 Bytes
IP Header	20 Bytes
AH Header	20 Bytes (at most)
ESP Header	40 Bytes (at most)
PPPoE Header	8 Bytes



Figure 11-17 IPsec Packet Format – Static IP/DHCP Internet Connection



Figure 11-18 IPsec Packet Format – PPPoE Internet Connection

Therefore, to avoid fragmentation in the IPsec switching path, the IPsec tunnel MTU should be smaller or equal to 1420 bytes ($1500 - 20 - 20 - 40 = 1420$) when the IPsec packets are sent over a static IP or DHCP Internet connection (see **Figure 11-17 IPsec Packet Format – Static IP/DHCP Internet Connection**); and it should be smaller or equal to 1412 bytes ($1420 - 8 = 1412$) when the IPsec packets are sent over a PPPoE Internet connection (see **Figure 11-18 IPsec Packet Format – PPPoE Internet Connection**).

On the UTT VPN gateway, the IPSec tunnel MTU is 1400 bytes by default. In most cases, please leave the default value because it can meet most application needs.

9.5.1.10 IPSec NAT Traversal

Network Address Translation (NAT) is a technology that allows multiple hosts on a private network to share a single or a small group of public IP addresses. Undoubtedly, NAT can help conserve the remaining IP address space and provide the benefit of network security assurance; however, it has introduced problems for end-to-end protocols like IPSec. NAT is incompatible with IPSec, which is one of the most popular VPN technologies.

Why doesn't NAT work with IPSec? One main reason is that NAT devices modify the IP header of a packet, this causes an AH-protected packet to fail checksum validation; and they cannot modify the ports in the encrypted TCP header of an ESP-protected packet. The solution is IPSec NAT Traversal, or NAT-T.

The IPSec working group of the IEEE has created standards for NAT-T that are defined in RFC 3947 (Negotiation of NAT-Traversal in the IKE) and RFC 3948 (UDP Encapsulation of IPsec ESP Packets). IPSec NAT-T is designed to solve the problems inherent in using IPSec with NAT.

During IKE phase 1 negotiation, the two IPSec NAT-T-capable endpoints can automatically determine:

- Whether both of the IPSec endpoints can perform IPSec NAT-T.
- If there are any NAT devices along the path between them.

If both of these two conditions are true, the two endpoints will automatically use IPSec NAT-T to send IPSec protected packets. If either endpoint doesn't support IPSec NAT-T, they will perform normal IPSec negotiations (beyond the first two messages) and IPSec protection. If both endpoints support IPSec NAT-T, but there is no NAT device between them, they will perform normal IPSec protection.



Note

IPSec NAT-T is only defined for ESP traffic. AH traffic cannot traverse NAT devices, therefore, do not use AH if any NAT device is present on your network.

The UTT VPN gateway supports IPSec NAT-T feature. With NAT-T, the UTT VPN gateway will add a UDP header to the ESP-protected packets after detecting one of more NAT devices along the data path during IKE phase 1 negotiation. This new UDP header sits between the ESP header and the outer IP header, and usually uses UDP port 4500.

*In the Web UI, you can go to the **VPN > IPSec > IPSec Settings** page to click the **Advanced Options** hyperlink to select the **Enable NAT-traversal** check box to enable IPSec NAT-T feature (section 6.1.2.2).*

9.5.1.11 IPSec Sessions Limit

The maximum number of concurrent IPSec sessions (i.e., tunnels) is depends on the specific product model. If the number of active VPN sessions has reached the maximum value, the system will reject any request for creating a new IPSec session and pop up a prompt dialog box shown in **Figure 11-19 Prompt Dialog Box – VPN Sessions Limit**.

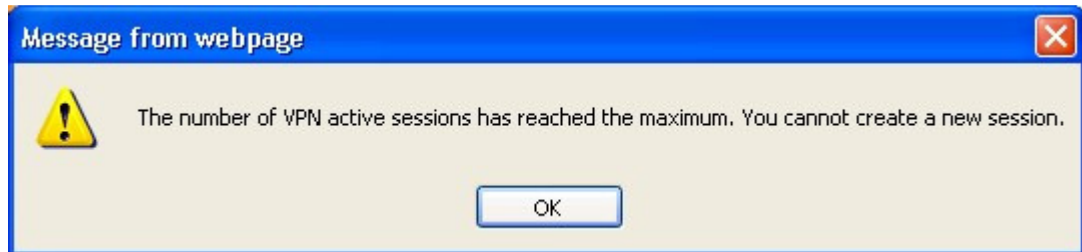


Figure 11-19 Prompt Dialog Box – VPN Sessions Limit

In the CLI, you can use the **show session history** command to view the related system log. As shown in **Figure 11-20 Viewing IPSec Sessions Limit Related System Log – CLI**, the log "Max VPN Sessions. Cannot set up a new IPSec session." means that the number of active VPN sessions has reached the maximum value, so you cannot create a new IPSec session.

```
04:13:18      Max VPN sessions.Cannot set up a new IPSec session.  
04:13:15      Ethernet Up
```

Figure 11-20 Viewing IPSec Sessions Limit Related System Log – CLI

In the Web UI, you can go to the **Status > System Log** page view the related system log. As shown in **Figure 11-21 Viewing IPSec Sessions Limit Related System Log – Web UI**, the log "Max VPN Sessions. Cannot set up a new IPSec session." means that the number of active VPN sessions has reached the maximum value, so you cannot create a new IPSec session.

```
04:13:18 Max VPN sessions.Cannot set up a new IPSec session.  
04:13:15 Ethernet Up
```

Figure 11-21 Viewing IPSec Sessions Limit Related System Log – Web UI

9.5.2 IPSec Settings–AutoKey (IKE)

In the **AutoKey (IKE)** mode, there are three connection types to choose: **Bidirectional**, **Originate-Only**, and **Answer-Only**. For each connection type, the configuration parameters are divided into two categories: basic and advanced parameters. Therein, the basic parameters for each type are different, but the advanced parameters are the same. The following will describe the basic parameters for each connection type respectively,

and then describe the advanced parameters for them.

1. Basic Parameters Settings

1) Bidirectional (Gateway-to-Gateway IPSec VPN)

If both IPSec endpoints have static IP addresses, you can choose **Bidirectional** as the connection type (see **Figure 11-22 IPSec Settings (AutoKey (IKE) – Bidirectional)**). In this case, the local UTT VPN gateway can act as an initiator or responder; and neither local ID nor remote ID is required.

IPSec Settings

Connection Type: Bidirectional

Remote

Gateway IP/Domain Name:

Subnet IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Local

Bind to: WAN1

Subnet IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Security Options

Pre-shared Key:

P2 Encrypt/Auth Algorithms: 1 (esp-aes128)

Figure 11-22 IPSec Settings (AutoKey (IKE) – Bidirectional)

- ◆ **Connection Type:** It specifies the role of the UTT VPN gateway in the IPSec tunnel establishment. The available options are **Bidirectional**, **Originate-Only** and **Answer-Only**. Here please select **Bidirectional**.
- ◆ **Gateway IP/Domain Name (Remote):** It specifies the IP address or domain name of the device at the other end of the IPSec tunnel. Note: If you enter a domain name, you should configure at least one DNS server on the UTT VPN gateway. Then the UTT VPN gateway will periodically resolve the domain name, and renegotiate the IPSec tunnel if the remote IPSec device's IP address changes.
- ◆ **Subnet IP and Subnet Mask (Remote):** They specify the remote subnet or host that can be accessed from the local side of the IPSec tunnel. If you want to define a

subnet, please enter any IP address belonging to that subnet in the **Subnet IP** text box and its mask in the **Subnet Mask** text box; if you want to define a host, please enter the IP address of that host in the **Subnet IP** text box and 255.255.255.255 in the **Subnet Mask** text box.

- ◆ **Bind to (Local):** It specifies an interface to which the IPSec tunnel is bound. The interface may be a physical interface, or PPPoE, PPTP or L2TP virtual interface. The IPSec module will check any inbound and outbound packets through this interface to decide if the packets require IPSec processing.
- ◆ **Subnet IP and Subnet Mask (Local):** They specify the local subnet or host that can be accessed from the remote side of the IPSec tunnel. If you want to define a subnet, please enter any IP address belonging to that subnet in the **Subnet IP** text box and its mask in the **Subnet Mask** text box; if you want to define a host, please enter the IP address of that host in the **Subnet IP** text box and 255.255.255.255 in the **Subnet Mask** text box.
- ◆ **Preshared Key:** It specifies a preshared key for IKE negotiation. It should be no more than 128 characters long. Note that you must enter the same preshared key at the remote IPSec device.
- ◆ **P2 Encrypt/Auth Algorithms 1:** It refers to the preferred phase 2 proposal that specifies a set of security protocols and algorithms for phase 2 negotiation.
- ▶ **Save:** Click it to save the IPSec settings.

2) Originate-Only (Dynamic-to-Static IPSec VPN)

If the local UTT VPN gateway has a dynamically assigned IP address, and the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a static IP address, you can choose **Originate-Only** as the connection type (see **Figure 11-23 IPSec Settings (AutoKey (IKE) – Originate-Only)**). In this case, the local UTT VPN gateway can only act as an initiator, and both IPSec endpoints should use aggressive mode for phase 1 IKE negotiation.

IPSec Settings

Connection Type Originate-Only ▼

Remote

Gateway IP/Domain Name

Subnet IP Address

Subnet Mask

ID Value

ID Type Domain Name ▼

Local

Bind to WAN1 ▼

Subnet IP Address

Subnet Mask

ID Value

ID Type Domain Name ▼

Security Options

Pre-shared Key

P2 Encrypt/Auth Algorithms 1 esp-aes128 ▼

Figure 11-23 IPsec Settings (AutoKey (IKE) – Originate-Only)

The parameters **Gateway IP/Domain Name (Remote)**, **Subnet IP (Remote)**, **Subnet Mask (Remote)**, **Bind to (Local)**, **Subnet IP (Local)**, **Subnet Mask (Local)**, **Preshared Key**, and **P2 Encrypt/Auth Algorithms 1** are the same as those in the **Bidirectional** connection type, please refer to the detailed descriptions of them.

The difference is that this connection type requires identity authentication. Specifically, the identity authentication for the local UTT gateway is required, that is, the local UTT gateway should provide its identity information to the remote IPsec endpoint for authentication; but the identity authentication for the remote IPsec endpoint is optional.

- ◆ **ID Type (Remote):** It specifies the type of remote ID. The available options are **Domain Name**, **Email Address**, **IP Address** and **Other**. In this connection type, it is an optional parameter. If you want remote IPsec device to be authenticated, please select one type and then specify **ID Value (Remote)**.
- ◆ **ID Value (Remote):** It specifies the identity of the remote IPsec device. In this connection type, it is an optional parameter. Please enter an ID value according to the selected **ID Type (Remote)**.

- ◆ **ID Type (Local):** It specifies the type of local ID. The available options are **Domain Name**, **Email Address**, **IP Address** and **Other**. In this connection type, it is a required parameter. You must select one type and then specify **ID Value (Local)** to allow the remote IPSec device to authenticate the local UTT VPN gateway.
- ◆ **ID Value (Local):** It specifies the identity of the local UTT VPN gateway. In this connection type, it is a required parameter. Please enter an ID value according to the selected **ID Type (Local)**.

3) Answer-Only (Static-to-Dynamic IPSec VPN)

If the local UTT VPN gateway has a static IP address, and the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a dynamically assigned IP address, you can choose **Answer-Only** as the connection type (see **Figure 11-24 IPSec Settings (AutoKey (IKE) – Answer-Only)**). In this case, the local UTT VPN gateway can only act as a responder, and both IPSec endpoints should use aggressive mode for phase 1 IKE negotiation.

IPSec Settings

Connection Type: Answer-Only

Remote

Gateway IP/Domain Name: 0.0.0.0

Subnet IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

ID Value:

ID Type: Domain Name

Local

Bind to: WAN1

Subnet IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

ID Value:

ID Type: Domain Name

Security Options

Pre-shared Key:

P2 Encrypt/Auth Algorithms: 1 esp-aes128

Figure 11-24 IPSec Settings (AutoKey (IKE) – Answer-Only)

The parameters **Gateway IP/Domain Name (Remote)**, **Subnet IP (Remote)**, **Subnet**

Mask (Remote), Bind to (Local), Subnet IP (Local), Subnet Mask (Local), Preshared Key, and P2 Encrypt/Auth Algorithms 1 are the same as those in the **Bidirectional** connection type, please refer to the detailed descriptions of them.

The difference is that this connection type requires identity authentication. Specifically, the identity authentication for the remote IPsec endpoint is required, that is, the remote IPsec endpoint should provide its identity information to the local UTT gateway for authentication; but the identity authentication for the local UTT gateway is optional.

- ◆ **ID Type (Remote):** It specifies the type of remote ID. The available options are **Domain Name, Email Address, IP Address** and **Other**. In this connection type, it is a required parameter. You must select one type and then specify **ID Value (Remote)** to allow the local UTT VPN gateway to authenticate the remote IPsec device.
- ◆ **ID Value (Remote):** It specifies the identity of the remote IPsec device. In this connection type, it is an optional parameter. Please enter an ID value according to the selected **ID Type (Remote)**.
- ◆ **ID Type (Local):** It specifies the type of local ID. The available options are **Domain Name, Email Address, IP Address** and **Other**. In this connection type, it is an optional parameter. If you want the local UTT VPN gateway to be authenticated, please select one type and then specify **ID Value (Local)**.
- ◆ **ID Value (Local):** It specifies the identity of the local UTT VPN gateway. In this connection type, it is a required parameter. Please enter an ID value according to the selected **ID Type (Local)**.

2. Advanced Parameters Settings

In the **Bidirectional** connection type, you should choose **Main** mode as the exchange mode for phase 1 IKE negotiation (see **Figure 11-25 IPsec Settings (AutoKey (IKE) – Advanced Options (Main Mode))**); in the **Originate-Only** or **Answer-Only** connection type, you should choose **Aggressive** mode (see **Figure 11-26 IPsec Settings (AutoKey (IKE) – Advanced Options (Aggressive Mode))**).

Phase 1

Exchange Mode Main ▼

SA Lifetime 28800 Seconds

Encrypt/Auth Algorithms 1 3des-md5-group2 ▼

Encrypt/Auth Algorithms 2 3des-sha-group2 ▼

Encrypt/Auth Algorithms 3 des-md5-group2 ▼

Encrypt/Auth Algorithms 4 des-sha-group2 ▼

Phase 2

Encrypt/Auth Algorithms 2 ----- ▼

Encrypt/Auth Algorithms 3 ----- ▼

Encrypt/Auth Algorithms 4 ----- ▼

SA Lifetime 3600 Seconds

Other Options

Enable Anti-replay ☐

Enable DPD ☐

Heartbeat Interval Seconds

PFS ☐

Enable NAT-traversal ☐

Port

Keepalive Frequency Seconds

Figure 11-25 IPSec Settings (AutoKey (IKE) – Advanced Options (Main Mode))

Phase 1

Exchange Mode	Aggressive ▼
SA Lifetime	28800 Seconds
Encrypt/Auth Algorithms 1	3des-md5-group2 ▼
Encrypt/Auth Algorithms 2	3des-sha-group2 ▼
Encrypt/Auth Algorithms 3	des-md5-group2 ▼
Encrypt/Auth Algorithms 4	des-sha-group2 ▼

Phase 2

Encrypt/Auth Algorithms 2	----- ▼
Encrypt/Auth Algorithms 3	----- ▼
Encrypt/Auth Algorithms 4	----- ▼
SA Lifetime	3600 Seconds

Other Options

Enable Anti-replay	☐
Enable DPD	☐
Heartbeat Interval	Seconds
PFS	☐
Enable NAT-traversal	☐
Port	
Keepalive Frequency	Seconds

Figure 11-26 IPSec Settings (AutoKey (IKE) – Advanced Options (Aggressive Mode)

- ◆ **Advanced Options:** Click this hyperlink to view and configure advanced parameters. In most cases, you need not configure them.
- ◆ **Exchange Mode:** It specifies the exchange mode used for IKE phase 1 negotiation. The available options are **Main** and **Aggressive**. If the **Connection Type** is **Bidirectional**, you should choose **Main** mode; else, you should choose **Aggressive** mode.
- ◆ **SA Lifetime (Phase 1):** It refers to IKE SA lifetime, which specifies the number of seconds (at least 600 seconds) an IKE SA will exist before expiring. A new IKE SA is negotiated 60 seconds before the existing IKE SA expires.

- ◆ **Encrypt/Auth Algorithms 1 ~ Encrypt/Auth Algorithms 4 (Phase 1):** They refer to phase 1 proposal that specifies a set of security algorithms for phase 1 negotiation. A phase 1 proposal includes an encryption algorithm, an authentication algorithm, and a DH group. You can choose up to four phase 1 proposals.
- ◆ **Encrypt/Auth Algorithms 2 ~ Encrypt/Auth Algorithms 3 (Phase 2):** They refer to phase 2 proposal that specifies a set of security protocols and algorithms for phase 2 negotiation. You can choose up to four phase 2 proposals together with **P2 Encrypt/Auth Algorithms 1**.
- ◆ **SA Lifetime (Phase 2):** It refers to IPSec SA time lifetime, which specifies the number of seconds (at least 600 seconds) an IPSec SA will exist before expiring. A new IPSec SA is negotiated 60 seconds before the existing IPSec SA expires.
- ◆ **Anti-replay:** It is used to enable or disable anti-replay. If you select this check box to enable anti-replay, the UTT VPN gateway can detect and reject replayed packets (i.e., old or duplicate packets) to protect itself against replay attacks.
- ◆ **DPD:** It is used to enable or disable DPD, which allows the UTT VPN gateway to detect an unresponsive peer. If you select this check box to enable DPD, the UTT VPN gateway will periodically send DPD heartbeat messages at the specified time interval (set by the **Heartbeat Interval**) to the remote IPSec device to verify its availability.
- ◆ **Heartbeat Interval:** It specifies a time interval (in seconds) at which the UTT VPN gateway will periodically send DPD heartbeat messages to the remote IPSec device to verify its availability.
- ◆ **PFS:** Perfect Forward Secrecy.
- ◆ **Enable NAT-traversal:** It is used to enable or disable NAT-traversal, which allows two IPSec devices establish an IPSec tunnel traverse one or more NAT devices.
- ◆ **Port:** It specifies the number of UDP port for NAT traversal. The default value is 4500.
- ◆ **Keepalive Frequency:** It specifies a time interval (in seconds) at which the UTT VPN gateway will periodically send keepalive packets to the NAT device to keep the NAT mapping active, so that the NAT mapping doesn't change until the IKE SA and IPSec SAs expire. This parameter will only take effect when NAT-traversal is enabled.

**Note**

IPSec provides two security protocols including AH and ESP for protecting data. AH is used to provide data authentication service. ESP is used to provide data encryption service, and/or data authentication service. The UTT VPN gateway supports both AH and ESP.

In addition, the UTT VPN gateway supports five encryption algorithms including DES, 3DES, AES128, AES192 and AES256, and two authentication algorithms including MD5 and SHA; it also supports Diffie-Hellman exchange including DH groups 1, 2, and 5 for

IKE phase 1 negotiation.

A phase 1 proposal consists of an encryption algorithm, an authentication algorithm, and a DH group; and there are five encryption algorithms, two authentication algorithms and three DH groups to choose. Therefore, there are thirty ($5 \times 3 \times 2 = 30$) phase 1 proposals supported. For example, the phase 1 proposal “3des-md5-group2” means that the encryption algorithm is 3DES, the authentication algorithm is md5, and the DH group is DH group 2.

In the Web UI, the UTT VPN gateway provides four phase 1 proposals by default; therefore, you need not configure phase 1 proposals in some cases. In addition, it allows you to configure phase 1 proposals as required. You can choose up to four phase 1 proposals in the Web UI, and twelve phase 1 proposals in the CLI.

A phase 2 proposal consists of one or two IPsec security protocols (either ESP or AH, or both), and algorithms used with the selected security protocol. ESP protects data with an encryption algorithm and/or an authentication algorithm, and AH protects data with an authentication algorithm. Therefore, there are fifty-three ($6 \times 3 \times 3 - 1 = 53$) phase 2 proposals supported. The details are as follows:

1. There are five phase 2 proposals for using ESP encryption only.
For example, the proposal “esp-des” means ESP encryption with DES algorithm.
2. There are two phase 2 proposals for using ESP authentication only.
For example, the proposal “esp-md5” means ESP authentication with MD5 algorithm.
3. There are two phase 2 proposals for using AH authentication only.
For example, the proposal “ah-sha” means AH authentication with SHA algorithm.
4. There are ten ($5 \times 2 = 10$) phase 2 proposals for using ESP encryption and ESP authentication.
For example, the proposal “esp-aes128-sha” means ESP encryption with AES128 algorithm and ESP authentication with SHA algorithm.
5. There are ten ($5 \times 2 = 10$) phase 2 proposals for using ESP encryption and AH authentication.
For example, the proposal “esp-aes192-ah-md5” means ESP encryption with AES192 algorithm and AH authentication with MD5 algorithm.
6. There are four ($2 \times 2 = 4$) phase 2 proposals for using ESP authentication and AH authentication.
For example, the proposal “esp-md5-ah-sha” means ESP authentication with MD5 algorithm and AH authentication with SHA algorithm.
7. There are twenty ($5 \times 2 \times 2 = 20$) phase 2 proposals for using ESP encryption, ESP authentication and AH authentication.
For example, the proposal “esp-aes256-sha-ah-md5” means ESP encryption with

AES256 algorithm, ESP authentication with SHA algorithm and AH authentication with MD5 algorithm.

By default, the UTT VPN gateway provides one phase 2 proposal by the parameter **P2 Encrypt/Auth Algorithms 1** (default value is esp-3des) in the Web UI. In addition, it allows you to choose up to four phase 2 proposals in the Web UI, and twelve phase 2 proposals in the CLI.

9.5.3 IPsec List

ID	Enable	SA Status	Remote Gateway	Remote Subnet	Bind to	Local Subnet	Edit
ID1	☒	Unestablished	200.200.200.200	192.168.1.1	WAN1	200.200.203.1	

☐ Select All

Figure 11-27 IPsec List

After you have finished configuring an IPsec entry, you can view its configuration and status information in the **IPsec List**, see **Figure 11-27 IPsec List**. The parameter definitions are as follows:

- ◆ **ID:** It is used to identify each IPsec tunnel in the list.
- ◆ **Enable:** Enable or disable the IPsec tunnel. The box is checked by default. You can disable the IPsec tunnel by checking off the box.
- ◆ **SA Status:** It displays the current status of the IKE SA and IPsec SAs. There are four kinds of status, see **Table 11-2 Description of IPsec SA Status**.

Status	Description
--------	-------------

Unestablished	The IKE SA and IPSec SAs are not established.
IKE Negotiating	IKE Phase 1 negotiation is in progress; the IKE SA is not established yet.
IPSec Negotiating	The IKE SA is established; IKE Phase 2 negotiation is in progress.
Established	The IPSec SAs are established.

Table 11-2 Description of IPSec SA Status

- ◆ **Remote Gateway:** It displays the IP address of the remote IPSec device.
- ◆ **Remote Subnet :** It displays the **Subnet IP (Remote)** you specify in the **VPN > IPSec > IPSec Settings** page.
- ◆ **Bind to:** It indicates the interface to which the IPSec tunnel is bound. If the IPSec tunnel is bound to a physical interface, it will display the physical interface's name (such as, eth2 refers to WAN1 interface); if the IPSec tunnel is bound to a PPPoE virtual interface, it will display the corresponding PPPoE connection's name; else, if the IPSec tunnel is bound to a PPTP or L2TP virtual interface, it will display the corresponding tunnel's ID.
- ◆ **Local Subnet :** It displays the **Subnet IP (Local)** you specify in the **VPN > IPSec > IPSec Settings** page.
- ▶ **Connect:** In the **AutoKey (IKE)** mode, the IPSec tunnel establishment can be triggered manually or by traffic. If you want to establish an IPSec tunnel manually, select the leftmost check box of the corresponding entry, and then click the **Connect** button.
- ▶ **Disconnect:** If you want to disconnect an established IPSec tunnel manually, select the leftmost check box of the corresponding entry, and then click the **Disconnect** button.

9.5.4 How to Add, View, Edit and Delete IPSec Entries

- ◆ **Add an IPSec Entry:** If you want to add an IPSec entry, click on **Add** button to go to setup page, and then configure it, lastly click the **Save** button.
- ◆ **View IPSec Entry(s):** When you have configured some IPSec entries, you can view them in the **IPSec List**.
- ◆ **Enable an IPSec Entry:** The **Enable** check box is used to enable or disable the corresponding IPSec entry. The default value is checked, which means the entry is in effect. If you want to disable the IPSec entry temporarily instead of deleting it, please

click it to remove the check mark.

- ◆ **Edit an IPSec Entry:** If you want to modify a configured IPSec entry, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ◆ **Delete IPSec Entry(s):** If you want to delete one or more IPSec entries, select the leftmost check boxes of them, and then click the **Delete** button.

9.5.5 Configuration Examples for IPSec – AutoKey (IKE)

As mentioned earlier, in the **AutoKey (IKE)** mode, there are three connection types to choose:

- **Bidirectional (Gateway-to-Gateway IPSec VPN):** Both IPSec endpoints have static IP addresses. In this case, the local UTT VPN gateway can act as an initiator or responder.
- **Answer-Only (Static-to-Dynamic IPSec VPN):** The local UTT VPN gateway has a static IP address, while the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a dynamic IP address. In this case, the local UTT VPN gateway can only act as a responder, and the remote endpoint should provide its identity information (such as an Email address, a domain name, etc) for authentication.
- **Originate-Only (Dynamic-to-Static IPSec VPN):** The local UTT VPN gateway has a dynamic IP address, while the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a static IP address. In this case, the local UTT VPN gateway can only act as an initiator, and it should provide its identity information (such as an Email address, a domain name, etc) to the remote endpoint for authentication.

9.5.5.1 Bidirectional (Gateway-to-Gateway IPSec VPN)

- If both IPSec endpoints have static IP addresses, you can choose **Bidirectional** as the connection type.

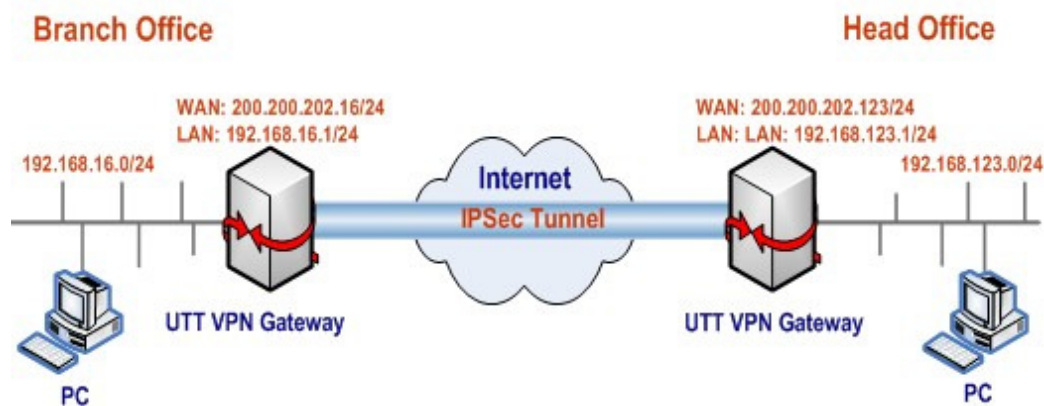


Figure 11-28 Network Topology – UTT VPN Gateway and UTT VPN Gateway (Bidirectional)

In this scenario (see **Figure 11-28 Network Topology – UTT VPN Gateway and UTT VPN Gateway (Bidirectional)**), we deploy two UTT VPN gateways at a company: one is located at the head office, and the other is located at the branch office. Now we want to use **AutoKey (IKE)** mode to establish an IPsec tunnel between them, and use the following proposals (i.e., encryption and authentication algorithms): the phase 1 proposals are left at their default values, and the preferred phase 2 proposal is esp-aes256-md5-ah-sha; in addition, the preshared key is testing, and the IP addresses are as follows:

The UTT VPN gateway at the head office:

- WAN Interface IP Address: 200.200.202.123/24
- Default Gateway IP Address: 200.200.202.254/24
- LAN Interface IP Address: 192.168.123.1/24

The UTT VPN gateway at the branch office:

- WAN Interface IP Address: 200.200.202.16/24
- Default Gateway IP Address: 200.200.202.254/24
- LAN Interface IP Address: 192.168.16.1/24

1. Configuring the UTT VPN gateway at the head office

Go to the **VPN > IPsec > IPsec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

Connection Type	Bidirectional
Gateway IP/Domain Name (Remote)	200.200.202.16
Subnet IP (Remote)	192.168.16.1
Subnet Mask (Remote)	255.255.255.0

Bind to (Local)	WAN1
Subnet IP (Local)	192.168.123.1
Subnet Mask (Local)	255.255.255.0
Preshared Key	testing
P2 Encrypt/Auth Algorithms 1	esp-aes256-md5-ah-sha

2. Configuring the UTT VPN gateway at the branch office

Go to the **VPN > IPSec > IPSec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

Connection Type	Bidirectional
Gateway IP/Domain Name (Remote)	200.200.202.123
Subnet IP (Remote)	192.168.123.1
Subnet Mask (Remote)	255.255.255.0
Bind to (Local)	WAN1
Subnet IP (Local)	192.168.16.1
Subnet Mask (Local)	255.255.255.0
Preshared Key	testing
P2 Encrypt/Auth Algorithms 1	esp-aes256-md5-ah-sha

3. Viewing the IPSec tunnel status

After you have configured IPSec parameters on both UTT VPN gateways, the IPSec tunnel establishment can be triggered manually or by traffic.

On the UTT VPN gateway, you can go to the **VPN > IPSec > IPSec List** page to view the configuration of the IPSec tunnel, including the **Remote Gateway**, **Remote Subnet IP**, **Bind to** and **Local Subnet IP**, see **Figure 11-29 IPSec List – UTT VPN Gateway and UTT VPN Gateway (Bidirectional)**. (here we take the UTT VPN gateway at the head office as an example). After the IPSec tunnel has been established, you can see that the **SA** **Status** displays **Established**.

IPSec List								
1/1 Lines/Page		10	First	Prev	Next	Last	Go to Page	Search
☐	ID	Enable	SA Status	Remote Gateway	Remote Subnet	Bind to	Local Subnet	Edit
☒	ID1	☒	Unestablished	200.200.202.16	192.168.16.1	WAN1	192.168.123.1	

☐ Select All

Figure 11-29 IPSec List – UTT VPN Gateway and UTT VPN Gateway (Bidirectional)

9.5.5.2 Answer-Only (Static-to-Dynamic IPSec VPN)

If the local UTT VPN gateway has a static IP address, and the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a dynamically assigned IP address (PPPoE or DHCP), you can choose **Answer-Only** as the connection type. In this case, the local UTT VPN gateway can only act as a responder, and both IPsec endpoints should use aggressive mode for phase 1 IKE negotiation.

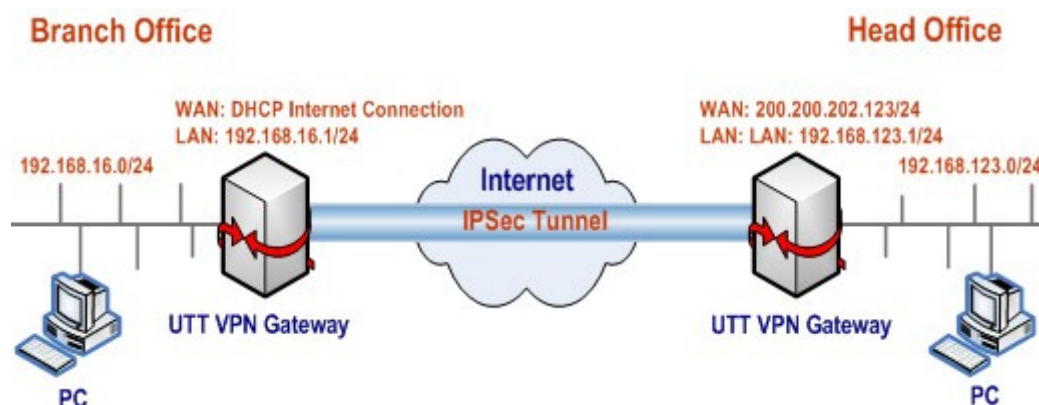


Figure 11-30 Network Topology – UTT VPN Gateway to UTT VPN Gateway (Answer-Only)

In this scenario (see **Figure 11-30 Network Topology – UTT VPN Gateway to UTT VPN Gateway (Answer-Only)**), we deploy two UTT VPN gateways at a company: one is located at the head office and connected to the Internet with a static IP address; the other is located at the branch office and connected to the Internet with a dynamic IP address (DHCP connection).

Now we want to use **AutoKey (IKE)** mode to establish an IPSec tunnel between them, and use the following proposals (i.e., encryption and authentication algorithms): the phase 1 proposals are left at their default values, and the preferred phase 2 proposal is esp-aes192-sha; in addition, the preshared key is testing, the originator's ID type is Email address and value is hiper@utt.com.cn, and the IP addresses are as follows:

The UTT VPN gateway at the head office:

- WAN Interface IP Address: 200.200.202.123/24
- LAN Interface IP Address: 192.168.123.1/24

The UTT VPN gateway at the branch office:

- WAN Interface IP Address: Dynamic (DHCP)
- LAN Interface IP Address: 192.168.16.1/24

1. Configuring the UTT VPN gateway at the head office

Go to the **VPN > IPSec > IPSec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

Key Mode	AutoKey (IKE)
Connection Type	Answer-Only
Gateway IP/Domain Name (Remote)	0.0.0.0
Subnet IP (Remote)	192.168.16.1
Subnet Mask (Remote)	255.255.255.0
ID Type (Remote)	Email Address
ID Value (Remote)	hiper@utt.com.cn
Bind to (Local)	WAN1
Subnet IP (Local)	192.168.123.1
Subnet Mask (Local)	255.255.255.0
Preshared Key	testing
P2 Encrypt/Auth Algorithms 1	esp-aes192-sha
Advanced Options	
Exchange Mode	Aggressive

2. Configuring the UTT VPN gateway at the branch office

Go to the **VPN > IPSec > IPSec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

Key Mode	AutoKey (IKE)
Connection Type	Originate-Only
Gateway IP/Domain Name (Remote)	200.200.202.123
Subnet IP (Remote)	192.168.123.1
Subnet Mask (Remote)	255.255.255.0
Bind to (Local)	WAN1
Subnet IP (Local)	192.168.16.1
Subnet Mask (Local)	255.255.255.0
ID Type (Local)	Email Address
ID Value (Local)	hiper@utt.com.cn
Preshared Key	testing
P2 Encrypt/Auth Algorithms 1	esp-aes192-sha
Advanced Options	
Exchange Mode	Aggressive

3. Viewing the IPSec tunnel status

After you have configured IPSec parameters on both UTT VPN gateways, the IPSec tunnel establishment can be triggered manually or by traffic.

On the UTT VPN gateway, you can go to the **VPN > IPSec > IPSec List** page to view the configuration of the IPSec tunnel, including the **Remote Gateway**, **Remote Subnet IP**, **Bind to** and **Local Subnet IP**, see **Figure 11-31 Responder's IPSec List – UTT VPN Gateway to UTT VPN Gateway (Answer-Only)** and **Figure 11-32 Initiator's IPSec List – UTT VPN Gateway to UTT VPN Gateway (Answer-Only)**. After the IPSec tunnel has been established, you can see that the **SA Status** displays **Established**.

1) Viewing the UTT VPN gateway at the head office

The following figure shows the configuration and status of the IPSec tunnel on the UTT VPN gateway with a static IP address at the head office.

IPSec List								
1/1 Lines/Page		10	First	Prev	Next	Last	Go to Page	Search
	ID	Enable	SA Status	Remote Gateway	Remote Subnet	Bind to	Local Subnet	Edit
☐	ID1	☒	Unestablished	200.200.202.16	192.168.16.1	WAN1	192.168.123.1	

☐ Select All
 Connect
Disconnect
Add
Delete All
Delete

Figure 11-31 Responder's IPSec List – UTT VPN Gateway to UTT VPN Gateway (Answer-Only)

2) Viewing the UTT VPN gateway at the branch office

The following figure shows the configuration and status of the IPSec tunnel on the UTT VPN gateway with a dynamic IP address at the branch office.

IPSec List									
1/1 Lines/Page		10		First	Prev	Next	Last	Go to Page	
					Search				
	ID	Enable	SA Status	Remote Gateway	Remote Subnet	Bind to	Local Subnet	Edit	
☐	ID1	☒	Unestablished	200.200.202.123	192.168.123.1	WAN1	192.168.16.1		

☐ Select All

Figure 11-32 Initiator's IPSec List – UTT VPN Gateway to UTT VPN Gateway (Answer-Only)

9.5.5.3 Originate-Only (Dynamic-to-Static IPsec VPN)

If the local UTT VPN gateway has a dynamically assigned IP address (PPPoE or DHCP), and the remote endpoint (another UTT VPN gateway or compatible VPN appliance) has a static IP address, you can choose **Originate-Only** as the connection type. In this case, the local UTT VPN gateway can only act as an initiator, and both IPsec endpoints should use aggressive mode for phase 1 IKE negotiation.

Please refer to section 12.2.5.2 for detailed information.

Chapter 10 System Administration

This chapter describes how to perform maintenance activities on the Gigabit Router, including administrator settings, system time settings, configuration backup and restore, firmware upgrade, remote management, and scheduled task settings.

10.1 Administrator

This section describes the **Administration > Administrator** page, where you can add, view, modify and delete the administrator accounts.

10.1.1 Administrator List

Administrator List

2/6

1/1
First
Prev
Next
Last
Go to Page
Search

	User Name	Edit
☐	admin	 
☐	test	 

☐ Select All

Add
Delete All
Delete

Figure 10-1 Administrator List

- ▶ **Add an Administrator Account:** To add a new administrator account, first click the **Add** button to go to the setup page, next configure it, lastly click the **Save** button.
- ▶ **View Administrator Account(s):** When you have configured one or more administrator accounts, you can view them in the **Administrator List**.
- ▶ **Modify an Administrator Account:** To modify a configured administrator account, click its **User Name** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete Administrator Account(s):** There are three ways to delete administrator account(s).

1. To delete an administrator account, directly click its  icon.
2. To delete more than one administrator account at a time, select the leftmost check boxes of the administrator accounts that you want to delete, and then click the **Delete** button.
3. To delete all the administrator accounts at a time, directly click the **Delete All** button.

 Note

You can change the default administrator password, but you cannot change its user name or delete it.

10.1.2 Administrator Settings



The form contains three input fields with red asterisks indicating they are required:

- User Name *
- Password *
- Confirm Password *

Below the fields is a note: "Note: To ensure security, it is strongly recommended that you change the default administrator password and keep it safe." At the bottom are three buttons: "Save", "Cancel", and "Back".

Figure 10-2 Administrator Settings

- ◆ **User Name:** It specifies a unique login name (case sensitive) of the administrator.
- ◆ **Password:** It specifies a login password (case sensitive) of the administrator. This password will be required to login to the Gigabit Router in the future.
- ◆ **Confirm Password:** You should re-enter the password.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Administrator List**.

 Note

To ensure security, it is strongly recommended that you change the default administrator password, remember your new password and keep it safe. Once changed, you should use the new password to login to the Gigabit Router in the future.

10.2 System Time

This section describes the **Administration > Time** page, see Figure 10-3.

To ensure that the time-related features (e.g., DDNS, Schedule, Access Control, etc.) work well, you should synchronize the system clock.

You can manually configure the system time or enable SNTP (Synchronize with SNTP Server) to automatically synchronize the system time from a designated SNTP server on the Internet. It is suggested that you choose SNTP to automatically synchronize time in most cases.

Current System Time Date 2011-12-17 Time 18:36:17

Time Zone UTC+0800 (Beijing, Chongqing, Hongkong, Urumchi) ▼

Set Time Manually ☐ Year 2011 Month 12 Day 17 18:36:17

Synchronize with SNTP Server ☒

SNTP Server 1 IP Address * 192.43.244.18

SNTP Server 2 IP Address * 129.6.15.28

SNTP Server 3 IP Address 0.0.0.0

Note: To ensure that SNTP operates properly, you should select the correct time zone.

Figure 10-3 System Time Settings

- ◆ **Current System Time:** It displays the Gigabit Router's current date (YYYY-MM-DD) and time (HH:MM:SS).
- ◆ **Time Zone:** It specifies the time zone for your local time. To ensure that SNTP operates properly, you must select the correct time zone.
- ◆ **Set Time Manually:** If you want to set the date (YYYY-MM-DD) and time (HH:MM:SS) for the Gigabit Router manually, select this radio button.
- ◆ **Synchronize with SNTP Server:** If you want the Gigabit Router to automatically synchronize the system clock from a designated SNTP server on the Internet, select this radio button.

- ◆ **SNTP Server 1 IP Address ~ SNTP Server 3 IP Address:** It allows you to configure up to three SNTP servers on the Gigabit Router. The Server 1 is the primary server (the default is 192.43.244.18), and the Server 2 is the first backup server (the default is 129.6.15.28), and the Server 3 is the second backup server (the default is 0.0.0.0).

- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.

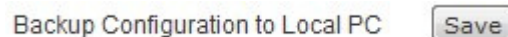
**Note**

For more information about SNTP, or to find an SNTP server with which you can synchronize the system clock, please refer to <http://www.ntp.org>.

10.3 Configuration

This section describes the **Administration > Configuration** page, where you can backup the current configuration file to the local PC, restore your previous configuration using the backup configuration file, and reset the Gigabit Router to factory default settings.

10.3.1 Backup Configuration



Backup Configuration to Local PC

Figure 10-4 Backup Configuration

- ▶ **Backup:** Click to export and save the Gigabit Router's current configuration to a text file on your local computer.

10.3.2 Restore Configuration



Restore Configuration

Reset to Factory Defaults before Restore ☐

Select a Configuration File

Figure 10-5 Restore Configuration

- ◆ **Reset to Factory Defaults before Restore:** If you select this check box, it will reset the Gigabit Router to factory default settings before importing the configuration file; else import the file directly.
- ◆ **Select a Configuration File:** Click the **Browse** button to choose an appropriate configuration file or enter the file path and name in the text box.
- ▶ **Restore:** Click to import the selected configuration file. It will overwrite the current configuration on the Gigabit Router with the new configuration.



Note

To avoid any unexpected error, do not power off the Gigabit Router during importing the configuration file.

10.3.3 Reset to Factory Defaults



Figure 10-6 Reset to Factory Defaults

- ▶ **Reset:** To reset the Gigabit Router to factory default settings, click the **Reset** button, and then restart the Gigabit Router.



Note

1. After performing the reset operation, you must manually restart the Gigabit Router in order for the default settings to take effect.
2. The reset operation will clear all of the Gigabit Router's custom settings. It is strongly recommended that you backup the current configuration before resetting.
3. The default administrator user name and password both are **admin** (case sensitive). The default LAN IP address is 192.168.1.1 with a subnet mask of 255.255.255.0.

10.4 Firmware Upgrade

This section describes the **Administration > Firmware** page, where you can view the current firmware version information, download the latest firmware from the website of UTT Technologies Co., Ltd., and upgrade the firmware.

The screenshot shows a web interface for firmware upgrade. At the top, 'Current Firmware Version' is displayed as 'nv520Wv1.0.0-111214'. Below this is a blue hyperlink 'Download Firmware'. Underneath is a text input field labeled 'Select a Firmware File' with a 'Browse...' button to its right. Below the input field is a checkbox labeled 'Restart after Upgrade' which is checked. At the bottom of the form is an 'Upgrade' button. Below the form, there are three lines of instructional text: 'Click "Download Firmware" to download the latest firmware from the UTT website.', 'Please select the appropriate firmware file according to the product model. You'd better go to System > Configuration to backup the Router's current configuration before upgrade.', and 'To avoid any unrecoverable error, Do NOT turn off the power.'

Figure 10-7 Firmware Upgrade

- ◆ **Current Firmware Version:** It displays the version of the current firmware installed on the Gigabit Router.

To upgrade the Gigabit Router's firmware, follow these steps:

Step 1 Downloading the latest firmware

Click the **Download Firmware** hyperlink to download the latest firmware from the website of UTT Technologies Co., Ltd.

Note

1. Please select the appropriate firmware file according to the product model.
2. It is recommended that you go to the **Administration > Configuration** to backup the Gigabit Router's current configuration before upgrade.

Step 2 Choosing the firmware

Click the **Browse** button to choose the firmware file you want to upgrade or enter the file path and name in the **Select a Firmware File** text box.

- ◆ **Restart after Upgrade:** After the upgrade is complete, the Gigabit Router will automatically restart in order for the new firmware to take effect.

Step 3 Renewing the firmware

Click the **Upgrade** button to renew the Gigabit Router's firmware. If you click the **Upgrade** button, you will be prompted to confirm the upgrade (see Figure 10-8). Then you can click **OK** to upgrade the firmware and restart the Gigabit Router, or click **Cancel** to cancel the operation.

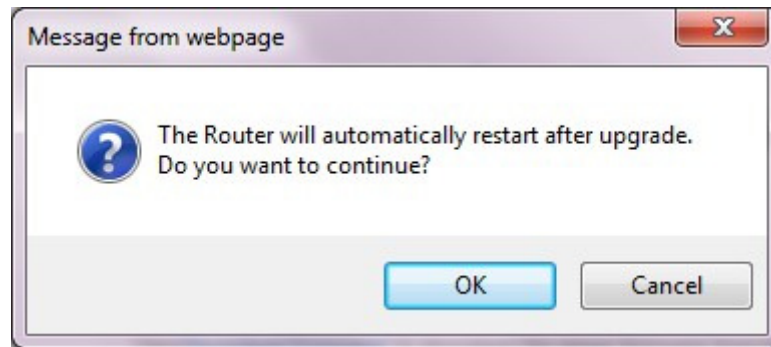


Figure 10-8 Prompt Dialog Box - Firmware Upgrade



Note

1. It is strongly recommended that you upgrade the firmware when the Gigabit Router is under light load.
2. If you upgrade firmware timely, the Gigabit Router will have more functionality and better performance. The right upgrade will not change the Gigabit Router's current settings.
3. To avoid any unexpected error or unrecoverable hardware damage, do not power off the Gigabit Router during upgrading.
4. After the upgrade is complete, the Gigabit Router will automatically restart in order for the new firmware to take effect, without human intervention.

10.5 Remote Access

This section describes the **Administration > Remote Access** page. In this page, you can enable HTTP remote management, which allows you to access the Gigabit Router's Web UI from anywhere over the Internet.

Enable HTTP ☐

If you select the check box, you can remotely access the Router's Web UI with the URL format: `http://IP address: port`.

Remote Management Port *

Interface

Note: To ensure security, you'd better not enable HTTP.

Figure 10-9 Remote Access Settings

- ◆ **Enable HTTP:** It allows you to enable or disable HTTP remote management. Select this check box to enable HTTP remote management. To access the Gigabit Router's Web UI over the Internet, you should enter **http://** and the Gigabit Router's WAN IP address, followed by a colon and the port number. For example, if the WAN IP address is 218.21.31.3 and port number is 8081, please enter <http://218.21.31.3:8081> in your browser's address bar.
- ◆ **Remote Management Port:** It specifies the port number that will be open to outside access. The default value is 8081.
- ◆ **Interface:** It specifies the interface on which the HTTP remote management is enabled. Here you can select only one interface. To enable HTTP remote management on multiple interfaces at the same time, you need to go to the **Advanced > NAT&DMZ > Port Forwarding** page to create port forwarding entry(s) for the other interface(s).
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.



Note

1. To ensure security, it is strongly recommended that you don't enable HTTP remote management unless necessary.
2. After you enable the HTTP remote management, the system will automatically create a port forwarding entry whose name is **admin**. You can go to the **Advanced > NAT&DMZ > Port Forwarding** page to view it in the **Port Forwarding List**.

10.6 Scheduled Task

This section describes the **Administration > Scheduled Task** page, where you can create and view the scheduled tasks. With scheduled tasks, the Gigabit Router can periodically start each task at the time you specify.

10.6.1 Scheduled Task Settings



Task Name * Task-1

Repeat Weekly

Start Time Monday 12 : 00 : 00

Task Content Restart

Save Cancel Back

Figure 10-10 Scheduled Task Settings

- ◆ **Task Name:** It specifies a unique name of the task.
- ◆ **Repeat:** It specifies how often the Gigabit Router will perform the task. The available options are **Weekly**, **Daily**, **Hourly**, **Minutely**.
- ◆ **Start Time:** It specifies the time at which the Gigabit Router will start the task. Its settings depend on the value of **Repeat**.
- ◆ **Task Content:** It specifies the content of the task. Now the Gigabit Router only provide one option: **Restart**, which means that the Gigabit Router will restart itself periodically.
- ▶ **Save:** Click to save your changes.
- ▶ **Cancel:** Click to revert to the last saved settings.
- ▶ **Back:** Click to go back to the **Scheduled Task List**.

10.6.2 Scheduled Task List

Scheduled Task List 1/5

1/1 First Prev Next Last Go to Page Search

	Task Name	Repeat	Start Time	Task Content
☐	Task-1	Weekly	Monday 12:00:00	Restart

☐ Select All Add Delete All Delete

Figure 10-11 Scheduled Task List

Scheduled Task List 1/5

1/1 First Prev Next Last Go to Page Search

	Repeat	Start Time	Task Content	Edit
	Weekly	Monday 12:00:00	Restart	 

☐ Select All Add Delete All Delete

Figure 10-12 Scheduled Task List (Continue)

- ▶ **Add a Scheduled Task:** To add a new scheduled task, first click the **Add** button to go to the **Scheduled Task Settings** page, next configure it, lastly click the **Save** button.
- ▶ **View Scheduled Task(s):** When you have configured one or more scheduled tasks, you can view them in the **Scheduled Task List**.
- ▶ **Modify a Scheduled Task:** To modify a configured scheduled task, click its **User Name** hyperlink or  icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- ▶ **Delete Scheduled Task(s):** There are three ways to delete scheduled task(s).
 1. To delete a scheduled task, directly click its  icon.
 2. To delete more than one scheduled task at a time, select the leftmost check boxes of the tasks that you want to delete, and then click the **Delete** button.
 3. To delete all the scheduled tasks at a time, directly click the **Delete All** button.

Chapter 11 Status

This chapter describes how to view the wired status and wireless status, the traffic statistics for each interface, and system information including the current system time, system up time, system resources usage information, firmware version, and system log.

11.1 System Status

This section describes the **Status > System Status** page, which include **Wired Status** and **Wireless Status**.

Wired Status		Wireless Status	
WAN1:			
Connection Type	PPPoE	Status	Connected
IP Address	114.62.0.46	Subnet Mask	255.255.255.255
Gateway IP Address	114.62.0.1	MAC Address	00:22:AA:A8:A7:83
Primary DNS Server	219.233.241.166	Secondary DNS Server	211.167.97.67
Up Time	0:5:17:50		
WAN2:			
Connection Type	DHCP	Status	Disconnected
IP Address		Subnet Mask	
Default Gateway		MAC Address	00:22:AA:A8:B1:94
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		
LAN:			
IP Address	192.168.1.1	Subnet Mask	255.255.255.0
MAC Address	00:22:AA:A8:9D:73		
Refresh			

Figure 11-1 System Status - Wired Status

Wired Status		Wireless Status	
3G:			
Connection Type	3G	Status	Disconnected
IP Address		Subnet Mask	
Gateway IP Address		MAC Address	
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		
APClient:			
Connection Type	DHCP	Status	Disconnected
IP Address		Subnet Mask	
Default Gateway		MAC Address	00:22:AA:A8:C5:B9
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		
Wireless LAN:			
Status	Enabled	Operation Mode	APClient Mode
SSID	UTT-HIPER_a89d73	Wireless Mode	11b/g/n Mixed
Channel	6	MAC Address	00:22:AA:A9:B0:1C
Refresh			

Figure 11-2 System Status - Wireless Status

- **Wired Status:** Refer to **Section 4.2.1 Wired Status** for detailed information.

**Note**

The **Wired Status** page and **Wireless Status** page only display the status information of the interfaces that have been configured.

9.5 Traffic Statistics

This section describes the ingress and egress traffic statistics for each interface.

WAN1:		Transmitted	Received
	Bytes	2305372	7971015
	Packets	10327	11409
.....			
WAN2:		Transmitted	Received
	Bytes	10626	0
	Packets	231	0
.....			
3G:		Transmitted	Received
	Bytes	0	0
	Packets	0	0
.....			
LAN:		Transmitted	Received
	Bytes	9780001	2604198
	Packets	11797	10647
.....			
		Clear	Refresh
		Back	

Figure 11-3 Traffic Statistics

- ◆ **WAN1, 3G, APClient and LAN:** You can view the traffic statistics for each interface, including the number of bytes received and transmitted, and the number of packets received and transmitted.

- ▶ **Clear:** Click to clear all traffic statistics.
- ▶ **Refresh:** Click to view the latest traffic statistics.
- ▶ **Back:** Click to go back to the **Start > Interface Traffic** page.

✓ **Note**

This page only displays the traffic statistics for the interfaces that have been configured.

11.3 System Information

This section describes the **Status > System Info** page, which includes the current system time, system up time, system resources usage information, SN, firmware version, and system log. System information can help you identify and diagnose the source of current system problems, or help you predict potential system problems.

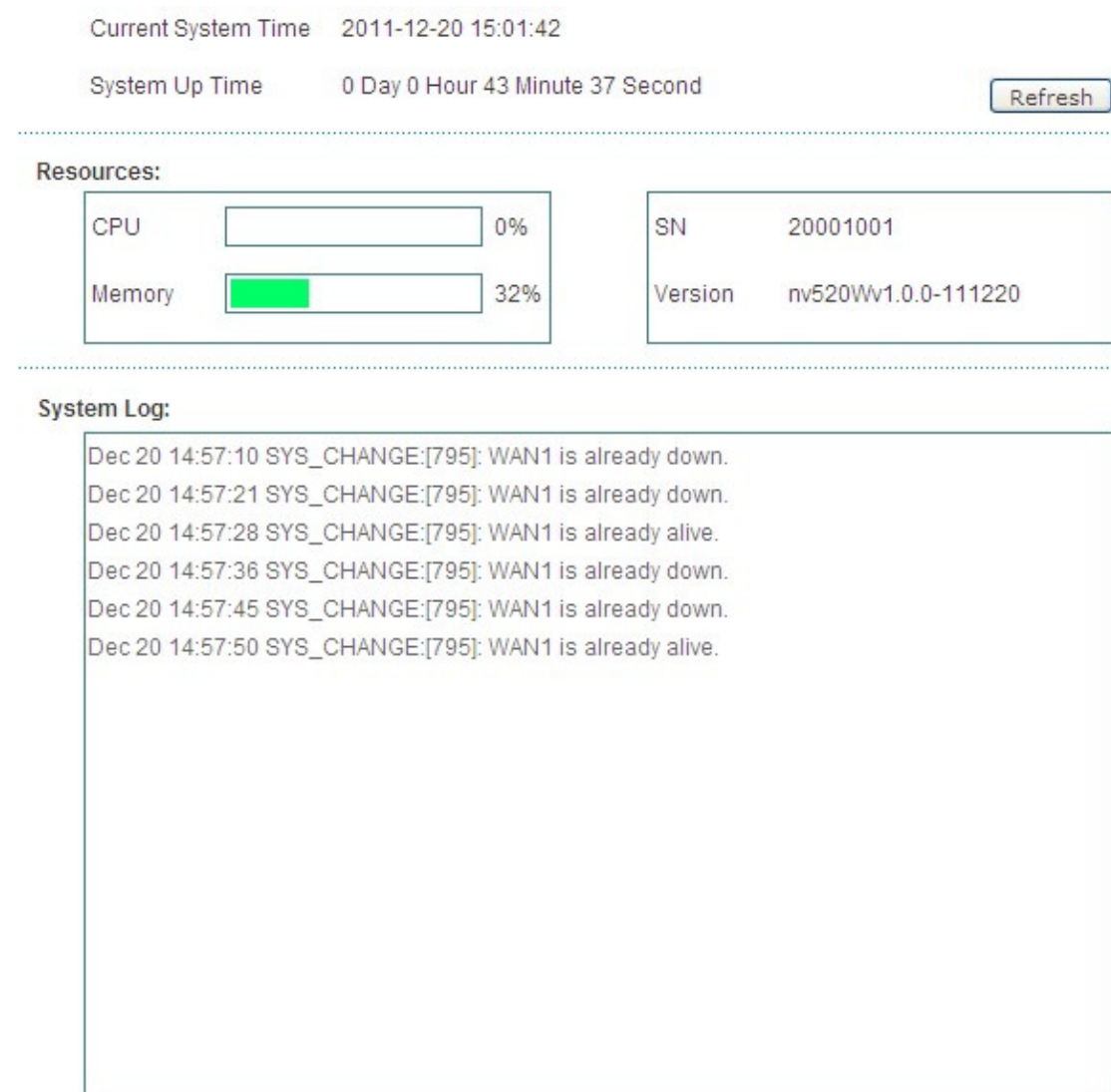


Figure 11-4 System Information

- ◆ **Current System Time:** It displays the Gigabit Router's current date (YYYY-MM-DD) and time (HH:MM:SS).
- ◆ **System Up Time:** It displays the elapsed time (in days, hours, minutes and seconds) since the Gigabit Router was last started.
- ◆ **CPU:** It displays the current CPU usage.
- ◆ **Memory:** It displays the current memory usage.

- ◆ **SN:** It displays the internal serial number of the Gigabit Router, which may be different from the SN found on the label at the bottom of the Gigabit Router.
- ◆ **Version:** It displays the version of the current firmware installed on the Gigabit Router.
- ◆ **System Log:** It records the events that occur in the system, such as, system startup, wireless enabled, and so on.
- ▶ **Refresh:** Click to view the latest system information.

**Note**

The **CPU** and **Memory** are displayed as a status bar and percentage value. The color of the status bar indicates the usage percentage for each resource.

- When the percentage is below 1%, the bar is blank.
- When the percentage is between 1% and 50% (below 50%), the color is green.
- When the percentage is between 50% and 70% (below 70%), the color is orange.
- When the percentage is equal to or above 70%, the color is red.

Chapter 12 Support

The **Support** page provides links to the UTTCare, Forum, Knowledge and Reservation page of the UTT website, which can help you quickly learn the UTT Technologies service system and enjoy the most intimate and professional services.

UTT Technologies, founded in 2000, is a leading provider of network service and solutions for small and medium-sized enterprises in China. The headquarters and the R&D center are located in Shanghai Caohejing Songjiang Hi-Tech Park with 12 branches located throughout China. UTT is a high-tech software company which gets major support from the state.

Technical Support Phone: +86-4006-120-780



Figure 12-1 Support

As shown in Figure 12-1, it allows you to click each **Learn More** hyperlink to directly open the corresponding page of the UTT website.

- **UTTCare:** Link to the support page of the UTT website to download product data and get help.
- **Forum:** Link to the forum page of the UTT website to participate in product discussions.
- **Knowledge:** Link to the knowledge base page of the UTT website to learn more about our products and how to use them.
- **Reservation:** Link to the booking customer service page of the UTT website to request a booking.

Appendix A How to Configure Your PC

This appendix describes how to configure TCP/IP settings on a Windows XP-based computer.

There are two ways to configure TCP/IP settings: manually configuring TCP/IP settings, and automatically configuring TCP/IP settings with DHCP. The following describes the two ways respectively.

- **Method One: Manually Configuring TCP/IP**

To configure the TCP/IP protocol manually, follow these steps:

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. Double-click the **Network Connections** icon, right-click the **Local Area Connection** icon and select **Properties**. On the **General** tab (see Figure A-0-1), in the **This connection uses the following items** box, click the **Internet Protocol (TCP/IP)** item, and then click the **Properties** button.

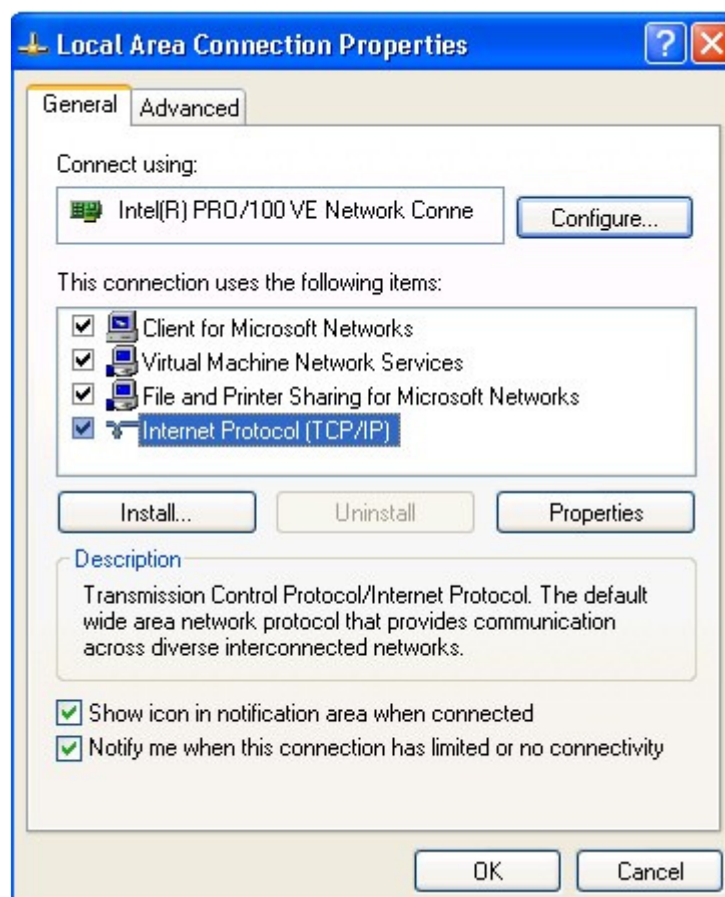
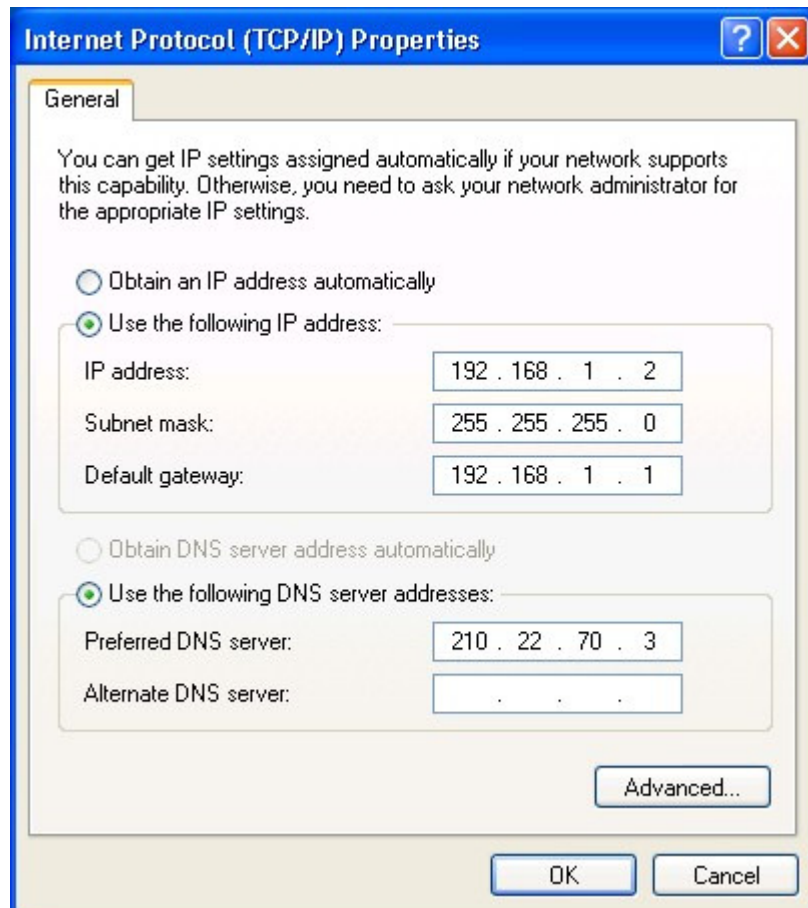


Figure A-0-1 Local Area Connection Properties

3. In the **Internet Protocol (TCP/IP) Properties** dialog box (see Figure A-0-2), select the **Use the following IP address** option, enter 192.168.1.x (x is between 2 and 254, including 2 and 253) in the **IP address** text box, 255.255.255.0 in the **Subnet mask** text box, and 192.168.1.1 in the **Default gateway** text box.

**Figure A-0-2 Internet Protocol (TCP/IP) Properties**

4. Select the **Use the following DNS server address** option, enter the primary DNS server IP address in the **Preferred DNS server** text box, and enter the secondary DNS server IP address in the **Alternate DNS server** text box (optional). A DNS query is sent to the primary DNS server at first. If the primary DNS server is unable to service the query, the query will be sent to the secondary DNS server.
5. Click the **OK** button. Now you have finished configuring the TCP/IP settings.

- **Method Two: Automatically Configuring TCP/IP with DHCP**

1. To ensure that the PC can obtain an IP address and other TCP/IP parameters automatically from the Gigabit Router, you should go to the **Network > DHCP Server** page to enable DHCP server on the Gigabit Router.

2. On the Windows taskbar, click **Start > Settings > Control Panel**.
3. Double-click the **Network Connections** icon, right-click the **Local Area Connection** icon and select **Properties**. On the **General** tab (see Figure A-0-1), in the **This connection uses the following items** box, click the **Internet Protocol (TCP/IP)** item, and then click the **Properties** button.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, on the **General** tab (see Figure A-0-3), select the **Obtain an IP address automatically** option and **Obtain DNS server address automatically** option.

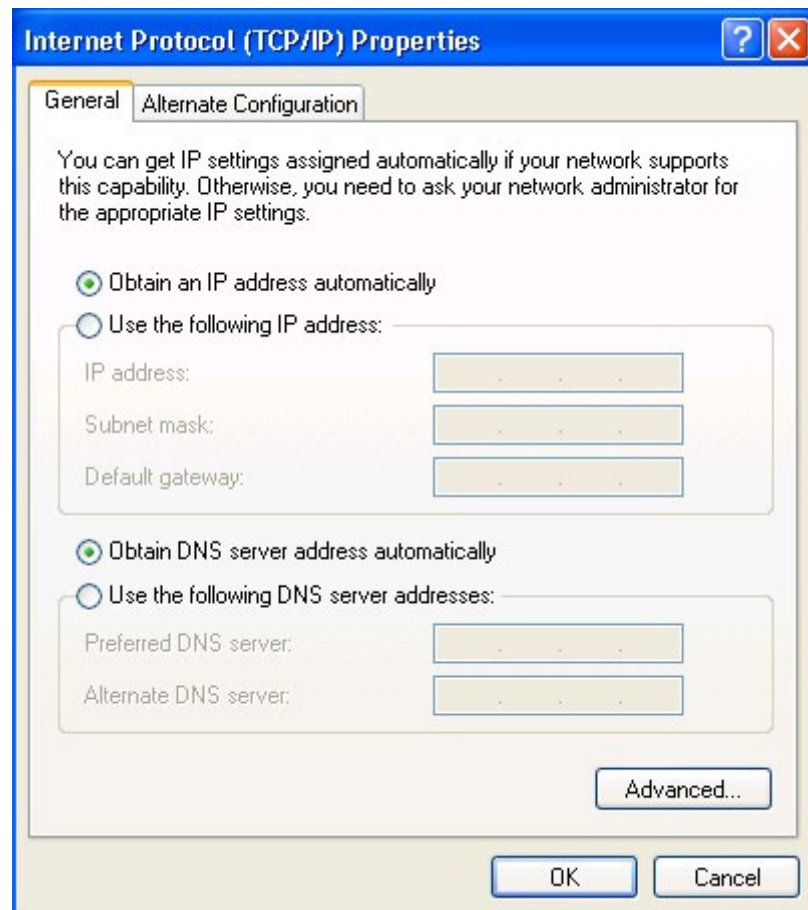


Figure A-0-3 Internet Protocol (TCP/IP) Properties

5. Click the **OK** button. Now you have finished configuring the TCP/IP settings.



Note

In Windows XP, the TCP/IP stack is a core component of the operating system. Therefore, you cannot remove TCP/IP in Windows XP. However, if you have network connectivity problems and think its TCP/IP related, you can reinstall TCP/IP on your Windows XP-based computer. To install TCP/IP on top of itself, follow these steps:

- a. On the Windows taskbar, click **Start > Settings > Control Panel**.
- b. Double-click **Network Connections**, right-click **Local Area Connection** and select **Properties**.

- c. Click **Install**.
- d. Click **Protocol**, and then click **Add**.
- e. Click **Have Disk**.
- f. In the **Copy manufacturer's files from** box, type **System_Drive_Letter:\windows\inf**, and then click **OK**.
- g. In the list of available protocols, click **Internet Protocol (TCP/IP)**, and then click **OK**.
- h. Restart your computer.

Appendix B FAQ

1. How to connect the Gigabit Router to the Internet using PPPoE?

- Step 1** Set your ADSL Modem to bridge mode (RFC 1483 bridged mode).
- Step 2** Please make sure that your PPPoE Internet connection use standard dial-type. You may use Windows XP built-in PPPoE dial-in client to test.
- Step 3** Connect a network cable from the ADSL modem to a WAN port of the Gigabit Router, and connect your telephone line to the ADSL modem's line port.
- Step 4** Configure the PPPoE Internet connection related parameters in the **Start > Setup Wizard** or the **Network > WAN** page.
- Step 5** If you pay monthly for the Internet connection, you can choose **Always On** as the **Dial Type**; else, you can choose **On Demand** or **Manual** as the **Dial Type**, and specify the **Idle Timeout** to avoid wasting online time due to that you forget to hang up the connection in time.
- Step 6** If you choose **Manual** as the **Dial Type**, you need to dial up manually in the **Internet Connection List** on the **Network > WAN** page. Refer to **Section 5.1.1.3** for more information.
- Step 7** After the PPPoE connection is established successfully, you can view its configuration and status information in the **Internet Connection List** on the **Network > WAN** page, such as **Status** (**Connected** means that the connection is established successfully), the connection's **IP address** and **Gateway** assigned by your ISP, **Tx Rate**, **Rx Rate**, and so on, see Figure B-0-1.

Internet Connection List

4/4

1/1

First

Prev

Next

Last

Go to

Page

Search

Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate
WAN1	PPPoE	Connected 2:46:5	114.62.0.95	255.255.255.255	114.62.0.1	17
WAN2	None					
3G	None					
APClient	None					

Delete

Connect

Disconnect

Refresh

Figure B-0-1 Viewing PPPoE Connection Status in the Internet Connection List

Internet Connection List							4/4
1/1	First	Prev	Next	Last	Go to	Page	Search
Status	IP Address	Subnet Mask	Default Gateway	Rx Rate (KB/s)	Tx Rate (KB/s)	Edit	
Connected 2:46:5	114.62.0.95	255.255.255.255	114.62.0.1	175	2		

Figure B-0-2 Viewing PPPoE Connection Status in the Internet Connection List (Continue)

Step 8 Configure the local computers according to the steps described in **Appendix A How to Configure Your PC**.

2. How to connect the Gigabit Router to the Internet using Static IP?

- Step 1** Please make sure the Internet connection is normal. You may use your PC to test.
- Step 2** Connect a network cable from the network device provided by your ISP to a WAN port of the Gigabit Router.
- Step 3** Configure the Static IP Internet connection related parameters in the **Start > Setup Wizard** or the **Network > WAN** page.
- Step 4** After the Static IP connection is established successfully, you can view its configuration and status information in the **Internet Connection List** on the **Network > WAN** page.
- Step 5** Configure the local computers according to the steps described in **Appendix A How to Configure Your PC**.

3. How to connect the Gigabit Router to the Internet using DHCP?

- Step 1** Please make sure the Internet connection is normal. You may use your PC to test.
- Step 2** Connect a network cable from the network device provided by your ISP to a WAN port of the Gigabit Router.

- Step 3** Configure the DHCP Internet connection related parameters in the **Start > Setup Wizard** or the **Network > WAN** page.



Note

Some ISPs register the MAC address of your network device (usually a computer) when your account is first opened, and they will only accept traffic from that MAC address. In this case, you need to change the new Router's MAC address to the registered MAC address. The operation is as follows: Go to the **Network > WAN** page, select the **MAC Address Clone** tab, and then change the MAC address of the corresponding interface, lastly click the **Save** button.

- Step 4** After the DHCP Internet connection is established successfully, you can go to the view its configuration and status information in the **Internet Connection List** on the **Network > WAN** page, such as **Status** (**Connected** means the connection is established successfully), the connection's **IP address** and **Gateway** assigned by your ISP, **Tx Rate**, **Rx Rate**, and so on, see Figure B-0-4.

Internet Connection List

4/4

1/1FirstPrevNextLastGo to PageSearch

Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate
WAN1	DHCP	Connected 1:31:20	114.62.7.194	255.255.255.255	114.62.0.1	1
WAN2	None					
3G	None					
APClient	None					

Delete

Connect

Disconnect

Refresh

Figure B-0-3 Viewing DHCP Connection Status in the Internet Connection List

Internet Connection List							4/4
1/1	First	Prev	Next	Last	Go to Page		Search
Status	IP Address	Subnet Mask	Default Gateway	Rx Rate (KB/s)	Tx Rate (KB/s)	Edit	
Connected 1:31:20	114.62.7.194	255.255.255.255	114.62.0.1	126	2		
							
							
							

Figure B-0-4 Viewing DHCP Connection Status in the Internet Connection List (Continue)

- Step 6** Configure the local computers according to the steps described in **Appendix A**
How to Configure Your PC.

4. How to reset the Gigabit Router to factory default settings?



Note

The reset operation will clear all the custom settings on the Gigabit Router, so do it with caution.

The following describes how to reset the Gigabit Router to factory default settings. There are two cases depending on whether you remember the administrator password or not.

- **Case One: Remember the administrator password**

When you remember the administrator password, you can reset the Gigabit Router to factory default settings via the Web UI. The operation is as follows: Go to the **Administration > Configuration** page, and then click the **Reset** button in the **Reset to Factory Defaults** configuration field, lastly manually restart the Gigabit Router.

- **Case Two: Forget the administrator password**

If you forget the administrator password, you cannot login to the Gigabit Router's Web UI. However, you can reset the Gigabit Router to factory default settings via the RESET button, which is located on the rear panel of the Gigabit Router. The operation is as follows: While the Gigabit Router is powered on, use a pin or paper clip to press and hold the RESET button for more than 5 seconds, and then release the button. After that, the Gigabit Router will restart with factory default settings.

Appendix C Common IP Protocols

Protocol Name	Protocol Number	Full Name
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
IPINIP	4	IP in IP Tunnel Driver
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Protocol
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocol
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhanced Interior Gateway Routing Protocol
OSPF	89	Open Shortest Path First

Appendix D Common Service Ports

Service Name	Port	Protocol	Description
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP, control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nickname	43	tcp	whois
domain	53	tcp	Domain Name Server

domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	udp	Bootstrap Protocol Client
tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtelnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nnrp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server

snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol
irc	194	tcp	Internet Relay Chat Protocol
ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	

conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login
kshell	544	tcp	Kerberos remote shell
new-rwho	550	udp	
remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol

radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server

Appendix E Figure Index

Figure 0-1 MAC Address Filtering List	3
Figure 2-1 Front Panel of the Gigabit Router	11
Figure 2-2 Back Panel of the Gigabit Router	13
Figure 3-1 Entering IP address in the Address Bar	17
Figure 3-2 Login Screen	17
Figure 3-3 Homepage.....	18
Figure 3-4 Running the Setup Wizard.....	19
Figure 3-5 Welcome Page	20
Figure 3-6 Setup Wizard - Internet Access Mode	错误！未定义书签。
Figure 3-7 Setup Wizard - WAN1 Internet Connection Settings (Static IP)	21
Figure 3-8 Setup Wizard - WAN1 Settings (DHCP).....	22
Figure 3-9 Setup Wizard - WAN1 Settings (PPPoE)	23
Figure 3-10 Setup Wizard - 3G Internet Connection Settings.....	错误！未定义书签。
Figure 3-11 Setup Wizard - APClient Connection Settings (Disabling Wireless Security)错误！未定义书签。	
Figure 3-12 Setup Wizard - APClient Connection Settings (WEP)	错误！未定义书签。
Figure 3-13 Setup Wizard - APClient Connection Settings (WPA-PSK/WAP2-PSK)错误！未定义书签。	
Figure 3-14 Setup Wizard - Wireless Settings	错误！未定义书签。
Figure 4-1 System Status - Wired Status.....	25
Figure 4-2 System Status - Wireless Status.....	26
Figure 4-3 Interface Traffic Chart	27
Figure 4-4 Traffic Statistics.....	28
Figure 4-5 Restart the Gigabit Router	29
Figure 4-6 Prompt Dialog Box - Restart the Gigabit Router	29
Figure 5-1 Internet Connection List.....	30
Figure 5-2 Internet Connection List (Continue).....	31
Figure 5-3 Internet Connection List - PPPoE/3G Connection	34
Figure 5-4 Internet Connection List - DHCP Connection.....	34
Figure 5-5 Network - WAN Settings.....	35
Figure 5-6 Static IP Internet Connection.....	36
Figure 5-7 DHCP Internet Connection Settings.....	36
Figure 5-8 PPPoE Internet Connection Settings	37
Figure 5-9 3G Internet Connection Settings	39
Figure 5-10 MAC Address Clone	40
Figure 5-11 Global Settings - Full Load Balancing	43
Figure 5-12 Global Settings - Partial Load Balancing	44
Figure 5-13 Load Balancing List	45

Figure 5-14 Load Balancing List (Continue)	45
Figure 5-15 Connection Detection Settings	46
Figure 5-16 LAN Interface Settings.....	48
Figure 5-17 DHCP Server Settings	49
Figure 5-18 Static DHCP Settings	51
Figure 5-19 Static DHCP List	52
Figure 5-20 DHCP Client List	53
Figure 5-21 DHCP Server Settings - Example.....	56
Figure 5-22 Adding the Static DHCP Entry 1 - Example	56
Figure 5-23 Adding the Static DHCP Entry 2 - Example	57
Figure 5-24 Static DHCP List - Example.....	57
Figure 5-25 Apply for a DDNS Account from 3322.org.....	59
Figure 5-26 Disabling DDNS Service.....	59
Figure 5-27 DDNS Settings Related to 3322.org.....	60
Figure 5-28 DDNS Settings Related to iplink.com.cn	61
Figure 5-29 DDNS Status	62
Figure 5-30 Enable UPnP	63
Figure 5-31 UPnP Port Forwarding List	64
Figure 6-1 Port Forwarding List	68
Figure 6-2 Port Forwarding Settings.....	69
Figure 6-3 Port Forwarding Settings - Example	71
Figure 6-4 NAT Rule List	71
Figure 6-5 NAT Rule Settings - EasyIP	72
Figure 6-6 NAT Rule Settings - One2One	73
Figure 6-7 EasyIP NAT Rule Settings - Example	75
Figure 6-8 One2One NAT Rule Settings - Example	77
Figure 6-9 DMZ Host Settings.....	77
Figure 6-10 IP/MAC Binding Global Settings.....	80
Figure 6-11 IP/MAC Binding List	81
Figure 6-12 Modifying an IP/MAC Binding.....	81
Figure 6-13 IP/MAC Binding Error Message	82
Figure 6-14 IP/MAC Binding Settings	82
Figure 6-15 IP/MAC Binding List - Example 1.....	85
Figure 6-16 IP/MAC Binding List - Example 2.....	86
Figure 6-17 IP/MAC Binding List - Example 3.....	86
Figure 6-18 Static Route List	87
Figure 6-19 Static Route Settings	88
Figure 6-20 Static Route Settings - Example	89
Figure 6-21 PPPoE Discovery Stage Flows	91
Figure 6-22 PPPoE Server Global Settings.....	93
Figure 6-23 PPPoE Account List	94
Figure 6-24 PPPoE Account Settings.....	95
Figure 6-25 PPPoE User Status List	96
Figure 7-1 Global Management Policy Settings	97

Figure 7-2 Updating Policy	98
Figure 7-3 Global Management Policy - Example.....	99
Figure 7-4 Group Management Policy List.....	100
Figure 7-5 Group Management Policy List (Continue)	100
Figure 7-6 Group Management Policy Settings	102
Figure 7-7 Group Management Policy Example - Policy 1	104
Figure 7-8 Group Management Policy Example - Policy 2	105
Figure 7-9 Group Management Policy Example - Policy 3	106
Figure 7-10 Group Management List – Example.....	106
Figure 7-11 Group Management List – Example (Continue)	107
Figure 8-1 Access Rule List	110
Figure 8-2 Access Rule List (Continue).....	110
Figure 8-3 Access Rule List (Continue).....	111
Figure 8-4 Access Rule Settings - IP Filtering	112
Figure 8-5 Access Rule Settings - URL Filtering.....	114
Figure 8-6 Access Rule Settings - Keyword Filtering.....	115
Figure 8-7 Access Rule List - Example 1.....	117
Figure 8-8 Access Rule List - Example 1 (Continue)	117
Figure 8-9 Access Rule List - Example 1 (Continue)	117
Figure 8-10 Access Rule List - Example 2.....	118
Figure 8-11 Access Rule List - Example 2 (Continue).....	118
Figure 8-12 Access Rule List - Example 2 (Continue)	119
Figure 8-13 Access Rule List - Example 3.....	119
Figure 8-14 Access Rule List - Example 3 (Continue)	120
Figure 8-15 Access Rule List - Example 3 (Continue)	120
Figure 8-16 Access Rule List - Example 4.....	121
Figure 8-17 Access Rule List - Example 4 (Continue)	121
Figure 8-18 Access Rule List - Example 4 (Continue)	121
Figure 8-19 Domain Filtering Global Settings.....	122
Figure 8-20 Domain Filtering Settings	122
Figure 8-21 Attack Prevention Settings	124
Figure 9-1 Typical Application of PPTP	125
Figure 9-2 PPTP Packet Flow	127
Figure 9-3 PPTP Packet Format - Static IP/DHCP Internet Connection.....	129
Figure 9-4 PPTP Packet Format - PPPoE Internet Connection.....	129
Figure 9-5 PPTP Client Settings	130
Figure 9-6 PPTP Client List	131
Figure 9-7 PPTP Client List (Continue).....	131
Figure 9-8 Network Topology - The Gigabit Router Acts as a PPTP client.....	132
Figure 10-1 Administrator List.....	134
Figure 10-2 Administrator Settings	135
Figure 10-3 System Time Settings	136
Figure 10-4 Backup Configuration	138
Figure 10-5 Restore Configuration	138

Figure 10-6 Reset to Factory Defaults	139
Figure 10-7 Firmware Upgrade.....	140
Figure 10-8 Prompt Dialog Box - Firmware Upgrade	141
Figure 10-9 Remote Access Settings.....	142
Figure 10-10 Scheduled Task Settings	143
Figure 10-11 Scheduled Task List.....	144
Figure 10-12 Scheduled Task List (Continue)	144
Figure 11-1 System Status - Wired Status.....	145
Figure 11-2 System Status - Wireless Status.....	146
Figure 11-3 Traffic Statistics	147
Figure 11-4 System Information	148
Figure 12-1 Support	150
Figure A-0-1 Local Area Connection Properties.....	152
Figure A-0-2 Internet Protocol (TCP/IP) Properties	152
Figure A-0-3 Internet Protocol (TCP/IP) Properties	153
Figure B-0-1 Viewing PPPoE Connection Status in the Internet Connection List.....	155
Figure B-0-2 Viewing PPPoE Connection Status in the Internet Connection List (Continue)	156
Figure B-0-3 Viewing DHCP Connection Status in the Internet Connection List.....	157
Figure B-0-4 Viewing DHCP Connection Status in the Internet Connection List (Continue)	157

Appendix F Table Index

Table 0-1 Common Button Descriptions.....	3
Table 0-2 Basic Elements and Features of the List.....	4
Table 0-3 Factory Default Settings.....	5
Table 2-1 Description of LEDs on the Front Panel.....	12
Table 2-2 Description of Ports on the Rear Panel.....	13
Table 2-3 Description of Components on the Rear Panel.....	13
Table 5-1 Description of PPPoE Connection Status.....	31
Table 5-2 Description of Static IP Connection Status.....	32
Table 5-3 Description of DHCP Connection Status.....	32
Table 5-4 Description of 3G Connection Status.....	32